Exhibit 1

Coalition Plaintiffs' July 1, 2021 Expert Disclosures

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

COALITION PLAINTIFFS'
EXPERT DISCLOSURES – OPENING REPORTS

Pursuant to Fed. R. Civ. P. 26(a)(2) and the Court's Scheduling Order, Plaintiff Coalition for Good Governance and Plaintiffs William Digges III, Laura Digges, Ricardo Davis & Megan Missett ("Coalition Plaintiffs") hereby disclose the following Experts' Opening Reports ("Reports"):

1. Declaration of Duncan Buell, attached hereto as Exhibit "A";

2. Declaration of Harri Hursti, attached hereto as Exhibit "B";

3. Affidavit of Logan Lamb, attached hereto as Exhibit "C";

4. Declaration of Kevin Skoglund, attached hereto as Exhibit "D"; and

5. Declaration of Philip B. Start, attached hereto as Exhibit "E".

Coalition Plaintiffs further state that the referenced Reports will be supplemented by further expert opinions that will be forthcoming as soon as possible

after Defendants have produced the numerous requested, but currently overdue and outstanding, discovery responses that are required by Coalition Plaintiffs' experts in order to formulate those forthcoming opinions.

This 1st day of July, 2021.

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Robert A. McGuire, III
Robert A. McGuire, III
Admitted Pro Hac Vice
(ECF No. 125)
ROBERT MCGUIRE LAW FIRM
113 Cherry St. #86685
Seattle, Washington 98104-2205
(253) 267-8530

Counsel for Coalition for Good Governance

/s/ Cary Ichter
Cary Ichter
Georgia Bar No. 382515
ICHTER DAVIS LLC
3340 Peachtree Road NE
Atlanta, Georgia 30326
(404) 869-7600

Counsel for William Digges III, Laura Digges, Ricardo Davis & Megan Missett

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on July 1, 2021, the undersigned caused a true and correct copy of the forgoing Coalition Plaintiffs' Expert Disclosures – Opening Reports, along with Exhibits A through E, to be served via email upon the following counsel of record:

Kaye Burwell
David Lowman
Cheryl Ringer
Fulton County Attorney's Office
141 Pryor Street, Suite 4038
Atlanta, Georgia 30303
kaye.burwell@fultoncountyga.gov
david.lowman@fultoncountyga.gov
cheryl.ringer@fultoncountyga.gov

David D. Cross
Lyle F. Hedgecock
Mary G. Kaiser
Veronica Ascarrunz
Eileen M. Brogan Jenna B. Conway
Robert W. Manoso
Morrison & Foerster, LLP
2000 Pennsylvania Avenue, NW
Washington, DC 20006
dcross@mofo.com
lhedgecock@mofo.com
mkaiser@mofo.com
vascarrunz@mofo.com
ebrogan@mofo.com

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,
Plaintiffs,

v.

BRIAN KEMP, ET AL.,
Defendants.

DECLARATION OF DUNCAN BUELL IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

Civil Action No. 1:17-CV-2989-AT

Pursuant to 28 U.S. § 1746, I, Duncan A. Buell, declare under penalty of perjury that the following is true and correct:

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I have been asked by counsel for Donna Curling, Donna Price, and Jeffrey Schoenberg to offer observations regarding the security of the DRE systems and their use in Georgia elections, based on my years of experience in the field of election security. I previously submitted an Affidavit on behalf of the Plaintiffs in this matter (Dkt. No. 15-2 Ex. G), a copy of which has been attached hereto as **Exhibit A**.

2. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University

of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell. My qualifications and experience are more fully set forth in **Exhibit A**.

3. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

4. I base the opinions in this Declaration on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

5. I have also used as a basis for my opinions a review of the documents regarding the KSU CES hack in Spring 2017, including those attached to the Affidavit of Logan Lamb (Dkt. No. 258-1 pp. 138-369).

6. In my experience working with electronic voting systems, one of the fundamental issues I have seen is the assumption among election officials that because a computer is being used, there is an additional level of protection that ensures accuracy and propriety of voting procedures. However, this is a false comfort. All software has inherent flaws, although some flaws are greater than others. Thus, it is important to understand the risks involved, to utilize programs that present the least risk, and, critically, to have in place procedures that further mitigate any risk present in the program selected. The prudent computing professional will always have in place procedures and practices to recover from the errors that we must always assume will happen. Based on my review of the material provided to me in this case to date, there is no indication that Georgia has followed these standard guidelines.

7. As a general matter, the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world with any interest or experience in election systems. The Diebold system has been scrutinized a number of times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has

been successful. As a result, there are serious, well-known risks associated with the use of the Diebold DREs used in Georgia.

8. One of the primary risks of the system is manipulation through the insertion of malware. Given the manner in which Georgia operates its elections through a central server, one need only access this central server in order to inject malicious code that could cause "disruption" (errors or failures) or "corruption" (the altering, addition, or deletion of votes) to a significant number of machines.

9. It is important to keep in mind that any malware injected does not have to be immediately executable, but can be written so as to execute only under certain conditions, perhaps only on Election Day, or otherwise tailored to meet the goals of the person attacking the system. Unfortunately, there is a wide array of coding techniques that could be employed to launch a targeted attack on a particular election, such as implementing a code to alter every one out of every 20 votes. In my experience, any sophisticated attack will likely involve multiple layers of code that are not only undetectable during an attack, but are "self-deleting" after they have been fully executed.

10. The risks of the DRE system software are exacerbated by the fact that there is no ability to audit results of any given election. As a result, in those instances in which there is a breach in protocol (whether intentional through one of

the methods set forth above or otherwise), there is often no way to determine the impact. The DRE system is able to count what was recorded, but there is no way to know if the vote as recorded by the DRE was what the voter intended. Thus, an attack is often undetectable, and the question of whether an attack actually had an impact on the election necessarily goes unanswered.

11. In addition to these general vulnerabilities, I understand that, as of late-2016, Georgia's central GEMS server was running a particular version of Drupal software that had well-known security vulnerabilities. Drupal is an open-source content-management system (CMS), meaning that it is a free product that has been modified by many people and used by many others. Over time, different versions of this software have presented different vulnerabilities. The specific version used by Georgia was subject to a vulnerability that resulted in what was aptly named Drupalgeddon, as it contained a well-known vulnerability to SQL Injection, which Drupal itself announced in October 2014.[1] Drupal warned that "a vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL injection .... This vulnerability can be exploited by anonymous users."[2]

---

[1] https://www.drupal.org/forum/newsletters/security-advisories-for-drupal-core/2014-10-15/sa-core-2014-005-drupal-core-sql

[2] *Id.*

12. SQL injection refers to a method of attack whereby a malicious user can insert code into forms on a website in order to have the website return a wide array of (often sensitive) data. SQL injection is the common culprit behind many well-known data breaches, including the breach of the Illinois voter registration system that occurred in June 2016, as a result of which approximately 90,000 voter registration records were estimated to have been compromised.[3]

13. Based on my review of documents, I understand that officials at the Center for Election Systems ("CES") at Kennesaw State University, who at the time were responsible for the state's central server, were made aware in October 2016 of the Drupal vulnerability that permitted ready access to Georgia voter registration databases, based on the access of information by Logan Lamb. (Dkt. No. 258-1 at 126.) Mr. Lamb appears to have exposed this vulnerability again in February 2017, as it had not been fixed by that time. (*Id.* at 127.)

14. In my experience, the lapse in security that permitted Mr. Lamb to access the server twice before change was implemented is simply inexcusable. It is a basic premise of network management to keep all software versions up to date, to monitor bug and vulnerability news lists so as to learn quickly of bugs and vulnerabilities, and to install any and all software patches or bug fixes as they

[3] https://www.intelligence.senate.gov/sites/default/files/documents/os-ssandvoss-062117_0.pdf.

become available. At the time Mr. Logan accessed the central server in October 2016, the Drupal SQL vulnerability had been reported nearly two years earlier. In my nine years as chair of the Department of Computer Science and Engineering at the University of South Carolina, with a year in that period when I served as Interim Dean of the college, I was the supervisor for the college's network systems administrator. I can attest that monitoring news lists for vulnerabilities was a routine and ongoing activity and that patches and updates were made as soon as they became available and reliable, even at the occasional cost of lost productivity due to small amounts of downtime.

15. The prudent and professional systems administrators, when alerted to the potential of an unknown vulnerability, will know that it is critical to respond quickly in order to validate the risk and take whatever steps necessary to correct the vulnerability. Based on my review of material provided to date, these steps were not taken until March 2017 at the earliest, and to date, I have not seen evidence indicating that the proper corrective steps have been taken.

Columbia, South Carolina
Dated: August 7, 2018

DUNCAN A. BUELL

EXHIBIT A

AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of the petition to void the June 20, 2017, election and to prohibit further use of Georgia's current DRE voting system..

2. In my opinion, the Diebold electronic voting system used in Georgia is vulnerable both to malicious interference and inadvertent error. The Diebold system in general has been put under technical scrutiny several times by technical experts, and each time there have been multiple concerns raised about security and reliability. In fact, each laboratory attempt to compromise DRE systems to change votes has been successful.

3. The possible stamp of approval (for a modified system?) given by the Kennesaw State University (KSU) Center for Election Systems (CES) does not in my opinion mitigate for use in Georgia the known flaws of the system. Indeed, the recent reports from the Kim Zetter article for *Politico* seem to demonstrate that the KSU CES has been either unable or unwilling to address security, privacy, and integrity issues even when they have been privately disclosed to the CES by credible cybersecurity professionals. The fact that the FOIA request of Mr. Garland Favorito yielded only three emails between CES and Mr. Logan Lamb and Mr. Christopher Grayson suggests further that CES might not have been taking seriously the security threats that were pointed out by Lamb and Grayson.

Qualifications and Relevant Employment History

4. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell.

5. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

6. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics

different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the U.S. intelligence community.

7. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

8. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

9. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued. When

the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well. I have obtained and analyzed the data from the 2012, 2014, and 2016 elections in South Carolina, and I have also analyzed ES&S DRE-voting system data in more limited quantities from Colorado, North Carolina, Pennsylvania, and Texas.

Basis for My Opinions

10. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

11. I have also used for my opinions a review of the documents surrounding the KSU CES hack in Spring 2017, including the report attached to an email on 24 April 2017 from Stephen Gay to Merle King.

The Diebold Election System Was Unacceptable for Use in the CD6 Election Held 20 June 2017

12. I begin with the fact that the security, reliability, and software quality flaws of the standard Diebold election system are well known to everyone in the computer security world who has an interest in election systems. The letter from Georgia citizens to Secretary of State (SoS) Brian Kemp on 10 May 2017 cites the security analysis of

Feldman, Halderman, and Felten. The GEMS central server software analysis by Ryan and Hoke, cited in the same letter, shows flaws in the central server. The fact that all analyses of the "standard" Diebold election system, even operated in intended conditions, have found major flaws should cause all Georgia voters to have grave concerns as to whether the known failings and vulnerabilities have been mitigated for use in Georgia elections.

13. Evidence indicates that the April 18 and June 20 Special Elections were conducted using a "non-standard" customized Diebold DRE voting system, with an unusual configuration, not tested by a federally accredited laboratory.

14. Even more alarming is the fact that the CES server containing crucial election programming files was known to be open to entry and manipulation in August 2016, and this glaring security problem had not been corrected even as late as March 1, 2017.

15. We must assume that the failure to secure the system and its data caused the already unreliable and unfit system unquestionably to be vulnerable to undetected attack. The system must be considered compromised and it is only prudent that the system must be considered to have been compromised from August 2016 through March 2017, and should not be used to conduct a public election.

16. It has been well-established in the computer security world that the Diebold election system, as configured for "standard" use, is unfit for use due to security and reliability concerns. In my letter/request to Secretary Kemp, serving as a technical advisor to the citizens of Georgia who had petitioned for the non-use of the Diebold

systems in the 20 June 2017 election, I asked for responses to the questions of security and reliability. If the standard system had been modified by CES, and that system had been re-certified, and one could rely upon the security credentials of the KSU CES, then one might have some limited confidence in the suitability of the Diebold system for use in elections in Georgia.

17. The response from Secretary Kemp has been tepid at best. His letter of June 5, 2017, does not address technical questions, and does not really address the questions posed by the electors of Georgia in their original request to him.

18. To be specific, the report of 18 April 2017, attached to Mr. Gay's email to Merle King, is damning in what it says and what it does not say. What we see as "successes" are only that the response to a security incident went well. This is essentially the statement that when law enforcement officials arrived at the barn, they found the door closed, and they found no horses inside the barn, but they had arrived quickly.

19. We see a number of issues in the 18 April 2017 report that indicate that the KSU CES security protocols were insufficient, and we find no commentary on any of those protocols that might have mitigated the damage.

20. I do not see that there are technical comments about successful, or positive, security measures that would have mitigated the potential damage done by the fact that the CES system was apparently open to attack for an extended period by any determined actor.

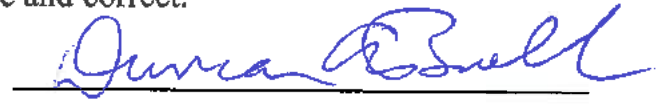
21. Indeed, the report can be read to suggest that the CES was not following some of the most basic security practices taught to all undergraduates in a computer

security course. Issues 1 and 8, under "Opportunities for Improvement", for example, cite a poor understanding of risk and of asset value on a main server and a failure to perform a security assessment. This apparent failure to know and to understand basic principles of security would not be inconsistent with Mr. Lamb's account that sensitive data was still openly available months after he had notified CES of this major security problem.

22. We come to the bottom line. We know, because it has been shown repeatedly, that the Diebold system as it is standardly configured, has major flaws. We would believe, based on our knowledge of process in Georgia, that it is the responsibility of the KSU CES to mitigate (or perhaps even remove?) these major flaws. But we do not see, in the report regarding the operational practices of the CES, that there is reason to believe that they have in fact mitigated the known flaws, produced a system that has been federally or state certified, and provided to the citizens of Georgia an election system in which they can be confident. For these reasons, the voting system in use cannot reasonably be approved as "safe and accurate for use" as required by Georgia statute.

23. For these reasons, I would argue that the Diebold system ought not be used in elections unless and until a complete security analysis has been performed on the software and hardware and a complete verification and integrity check has been made of the databases, including voter registration databases. Nor should the reported results generated by the system be relied on for a determination of the outcome of the June 20 special election.

24. I affirm that the foregoing is true and correct.



DUNCAN BUELL Date

Sworn before me this 29th day of June, 2017, in Columbia, SC.

Rebecca Mayo
NOTARY PUBLIC

EXHIBIT B

SUPPLEMENTAL DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. My background and qualifications in voting system cybersecurity are set forth in my December 16, 2019 declaration. (Doc. 680-1, pages 37 *et seq*). I stand by everything in that declaration, my August 21, 2020 declaration. (Doc. 800-2), and my August 24, 2020 declaration (Doc. 809-3)

Responses to State's Assertions

1. While the State attempts to minimize my experience with the Dominion Voting System used in Georgia, there are only a few independent voting system researchers with more hands-on experience than I have with key components of the Dominion Voting System elements. To my knowledge, no jurisdiction has permitted, and Dominion has not permitted, independent research, academic or otherwise, to be conducted on its systems, which greatly limits the number of people with any experience with the Dominion system.

2. For the last 4 years I have co-organized the DEF CON Voting Machine Hacking Village, which I co-founded. DEFCON in one of the oldest and largest annual security and hacker community meetings, attracting in 2019 over 30,000 participants into Las Vegas.

3. In the Voting Machine Hacking Village at DEF CON 27, we had a Dominion ImageCast Precinct device available for studying. In the publicly available DEF CON Voting Machine Hacking Village Annual Report of 2019, we outline on pages 18 and 19 the security weaknesses, vulnerabilities and exploitations of those discovered by the participants. Intentionally, the report does not disclose to the public the details of how the exploits were constructed, but rather provides a high-level overview of the discoveries. The underlining significance is that the people studying the machine had no prior knowledge or documentation of the system and yet achieved all discoveries in under 20 hours of working time. As co-organizer of the Village, I personally kept myself up to date with their work, including discoveries and details which were not reported in the annual report.

4. The State appears to challenge my opinion that the voting system server had not been hardened. (Doc. 834 at 5-6) My statements about the failure to harden the system and the accompanied pictures were referring to the Election Management and Tabulation Servers, specifically in Fulton County.

5. I declared that the servers *appeared* to not be hardened since at the time the only limited evidence available was my visual observation of device's user interface from a distance. The process of testing hardening is called penetration testing, which is a standard security practice. Subsequently, through Coalition Plaintiffs' discovery, on August 25, I obtained partial and time-limited event log files for both August 11th and August 25th.

6. A review and preliminary analysis of the log entries has since confirmed that services which would had been disabled in the hardening process are running on the server. The EMS server system logs I reviewed confirmed that services enabling remote access to the system entered into the running state on the EMS server. However, security log entries were are not available; these entries would have shown if remote access features were used. Fulton's EMS event log files for August 11th have a cut-off point at 17:31:50. The logs seem to be configured to run with maximum size, and then the log rolls over and the older log entries are lost. For example, one security log has 33,671 entries, and the first one is from 17:02:29, covering merely 29 minutes and 21 seconds of activities. This is a completely unacceptable practice. No acceptable practices would flood the security log this way. For example, at 17:03:49, a single second consisted of 258 security log entries of which 127 were consecutive logoff messages for ending sessions. This is called log flooding, and while it could be a result of

misconfiguration, it should always be investigated as an indication of irregularities, because, among other causes, it is a known method for attackers to destroy evidence.

7. I stand by my statement that the lack of security logs further strengthens my professional opinion of no confidence in the operations of the August 11th vote count, because the most basic feature of system security is missing-- an audit trail. The Windows log system is designed to split different entries into separate logs, and one log missing in most cases degenerates the value of all. The most basic security practices mandate maintaining and protecting reliable security logs, and this standard practice is not specific to election security. These are standard minimum practices which are essential parts of any good security practice in any system requiring cybersecurity.

Scanner and Tabulation Software Issues

8. I believe there is confusion in Georgia's election security conversation between the terms: scanner settings and election software vote-mark thresholds. Those are two separate settings, processed by separate software. Scanner settings do not affect image processing within the election software. Scanner settings are used by TWAIN API to configure the scanner and contain parameters which are of paramount importance when the thresholds are applied to produce a 1-bit image. The Dominion ballot image is a 1-bit image.

9. Election software processing starts from that 1-bit image (also known as “bi-level image”, and thresholds used to determine the mark thresholds are applied to that image. As the original image and majority of the information captured by the scanner is permanently lost in the conversion into a 1-bit image, the election software settings cannot overrule the scanner settings, but the scanner settings can de facto overrule the effectiveness of the election software settings. EXHIBIT E to my August 24 declaration shows the user instructions and a picture of the interface used by the user to verify and select scanner settings. The voter mark threshold value is not part of this user interface, as that is applied later in the election software against the images. The method of storing and applying the later values, inside a database or without, are irrelevant. The process of acquiring the image and preprocessing is separate and a precursor in election software activities.

10. The images obtained from Fulton County via Coalition Plaintiffs’ discovery make it clear that the ballot scanner itself does not process the ballot with fixed values in image processing prior to the election software. This is evident from Exhibit A. These are scanning the printed ovals on the paper ballots – as these are industrially produced in a printing process of the ballot, there should be no difference whatsoever how the scanner images those black ovals.

11. However, as the examples show, not even the identical printed ink registers uniformly the same on the ballots – and therefore neither will the vote the

voter casts. This also demonstrates one of the reasons why fixed threshold values alone for election software vote mark determination cannot solve the problem as the State Election Board is attempting to do. These values would be applied against the input image, which is not reliably reflecting the markings on the paper ballots. The scanner does not produce uniform images from the ballots. The root cause of this behavior is unclear.

12. Any attempt to merely re-bracket the thresholds (as the State Election Board is attempting) to a seemingly more reasonable standard without considerable research will continue to result in valid votes not being counted because of poor quality images are being used as the source document for electronic counting.

Explanation of Ballot Scanning Technology

13. The modern scanner does not take a picture of the paper. It illuminates the paper with 3 different colors - in essence taking 3 separate gray-scale images from the paper in different lighting. The next step is to combine, in software, these 3 images by assigning colors into the gray-scales and processing those to create an approximation of what the human eye would had seen. While the scanner observes red, green and blue equally, the human eye does not. The human eye is more sensitive to green than other colors and therefore the software is not taking the image as reported by the sensors, but processing that image to

correspond the human eye. This phase of the process includes many algorithms to create the image and clean the image by removing artifacts.

14. The resulting color image can be converted to gray-scale image and further to 1-bit, bi-level, black-or-white images. In this phase colors are again assigned values. Even darkest of yellow is not black, but darkest of blue can be very close to black. With these values, the colors are collapsed into values from 0 to 255 representing how relatively dark the human eye would see the color. The last step is typically just further cutting the into black-or-white by assigning white to all pixels under 50% gray and black to over 50% gray. As a result, a marking which is unquestionably clear to human can end up to be plain white, that is, no visible marking at all.

15. By the late 1970s, this 1-bit bi-level image processing was found unacceptable with early fax machines. To compensate the loss of image information, fax machines employed a technique called rastering to emulate gray-scales in 1-bit images. However, Dominion ballot image files do not employ this long available technique to compensate the effects loss of data.

16. I shall describe how dynamic settings adjust contrast in the grayscale and wash out information from the 1-bit image as a result. Historically, very often the documents being scanned are not originals, but were photocopies of the originals or copies of the copies. To improve the quality of pre-deteriorated

material, dynamic settings for brightness and contrast were developed to "wash out" the defects caused by copying, like white background not being white and black not being black and a variety of speckles that appear across the paper. In essence, the goal is to make the text easier to read by the human eye by removing anomalies and weaker markings. When this kind of techniques are applied and then the image converted to black-or-white pixels, the image becomes brittle, and intentional markings being lost.

17. While this process is useful for making text on this page easier to read, it can degrade human markings on a ballot. The human brain with the experience recognizes the markings better, when excess markings are removed – in contrast, Dominion software utilizes no intelligence and merely tries to calculate a value to make the determination. Therefore, this family of image enhancement features is not compatible with the approach chosen by the developers of the Dominion system.

18. Excerpts of the ballot vote targets in the Exhibit A are not degenerated as result of production for this document. These are degenerated this way in the original images obtained from Fulton County. While it is unclear what caused the failure to scan the vote target identically from identical sources, this kind of quality difference between documents is typical for dynamically adjusting

parameters. When the input material is not uniform, it cannot be measured in later process with fixed thresholds.

Fulton County Election Preparation Center August 25 observations

19. I visited the Fulton County Election Preparation Center ("EPC") on August 25 from 10:50am to approximately 5pm. I had visited the Center multiple times and am generally familiar with their equipment configuration.

20. I was at EPC to conduct scanner testing using the original voter marked ballots that were rejected for scanning and hand duplicated in the June 9, 2020 election, as agreed with Fulton County in the discovery process. I was accompanied by Marilyn Marks and later in the afternoon by Rhonda Martin, of Coalition for Good Governance.

21. The Dominion technician (Dominic) had full operating control of the system as he had before during my visits on August 11 and August 17. Fulton County employees seem to have little to do with operating the server component of the system and little familiarity with it.

22. The failure of accountable election officials to have direct control of the voting system with proper administrative controls that prevent vendors and third parties from accessing the system is a troubling sign to voting system security

experts. Allowing vendors to operating voting systems greatly exacerbates the already lax security conditions and insider risks.

23. Before the scanning of the ballot started, Dominion technicians pulled up a new scanner options screen on the server monitor. I had not seen that screen before, nor had I seen references to it in the Dominion system documentation.

24. The computer driving the high-volume mail ballot scanner has a different Windows configuration than other election tabulation servers I observed before at EPC. This further elevates the suspicion that in addition to lack of system hardening, version management of the operating system has not been performed.

25. The high-volume ballot scanner scanned between 64 and 70 ballots per minute on the longer uninterrupted runs.

26. When Dominic tried to upload scanned ballots from the ICC (high volume) scanner computer to the central tabulation computer, the same or very similar issues observed August 11 and August 17 repeated starting 11:40 am. (Exhibit B)

27. Dominic and other staff members started reading screen logs recorded on August 11 to understand what had happened. On the election night when I was observing the operations, Dominic was not involved with the troubleshooting, as he was performing operations with IPC uploads. The server logs I was provided through discovery revealed that the issue had already happened August 11 earlier

than I observed on the Election night. The logs revealed that operators had attempted to process ballot images for a period of time ending at 5:31:50 pm, and the same issues had appeared then too. Due to the fact that the logs end at 5:31:50 pm, I cannot compare the logs to the errors I observed on the election night. (Exhibit C)

28. The system operators were comparing log entries for August 11 and August 25. I got the clear impression that the issue had appeared on August 11 more than once, and was encountered on August 11 before I arrived to observe. The logs I reviewed revealed repeated errors of this nature.

29. The privileges observed on the screen reveal that Dominion staff members operating the server have privileges to delete individual log events and filter log entries for selective saving. This means that the logs produced now cannot be trusted to accurately reflect the history of transactions on the server. The most basic security practice is to never let the operators have privileges to delete or alter log events, because that makes supervision impossible and performing forensics difficult, if not impossible. In addition, trustworthy logs are essential to detect and deter malicious software or intrusion.

30. In the troubleshooting efforts, Dominic opened a Windows command line window. This told me that he has a level of sophistication typical for power users.

31. The troubleshooting followed the same trial-and-error pattern until 12:15pm. At that time, a Dominion employee again walked behind the rack and rewired something and inserted an USB stick behind the server. After rewiring, the Doninon employees started using the same screen as previously used as the main operating computer to access and directly interact with the main server on the rack. This server appeared to have yet another Windows configuration, and potentially version. (Video Exhibit E shows that the operations behind the rack cannot be observed and Exhibit F shows the new screen layout consistent with Windows Server user interface and distinctly different from Windows 10)

32. In the troubleshooting, the user list was displayed, and the list included account "Guest," which is one of the first things removed when a server is hardened. It is possible that the account has been disabled, but the standard practice is to remove the account to ensure that it will not get inadvertently reactivated in the future. (Exhibit G)

33. Dominic opened a text file containing the key passwords into the election system which was visible on the screen. It is completely unacceptable practice to have the passwords stored in clear text in the very system which is protected by the passwords in question. This is like posting the combination of a safe in a Post-it notes on safe door. This further reinforces the conclusion that even

the most basic security principles and best practices are ignored in Fulton County's election server operation. (Exhibit H – the actual passwords blurred)

34. Dominion staff wound down their efforts to troubleshoot the issue.

35. I requested the images of the test ballots that we had created on the scan test on August 17. Those images were created by the IPC (precinct) scanner we were using. Dominic, the Dominion employee, offered the excuse that the scanner does not record images and showed me server directory with no images. I countered him, telling him that the scanner needs to capture images in order to be able to process barcodes (votes). I furthermore pointed out that he had on August 17 loaded the memory card without checking "load images" option. He showed the dialog box, and "load images" was unchecked and when I asked him to check the box, it turned on. At Exhibit I is a photograph I took of the unchecked boxes showing the options of loading only results or images and audit logs as well.

36. When I asked if he could now reload the memory card with our test ballots, he refused to do so, telling me that he been trained to only load results on the server from the card and not to load the images or the audit logs of the precinct scanners. He further explained that he will load the images only if "his boss from Dominion" tells him to do so and recommended that someone call his boss.

37. From this point on, it become clear that Dominic (Dominion staff) was considered to be in charge of the election server operation and accepted

commands only Dominion management, not Fulton election officials. He repeated the same to county officials saying, "if I am told by my boss to do so, then I will".

38. And around 1 pm we left for lunch while Dominic stated that he had to go visit the Dominion office to get help with the loading of images.

39. When we returned, the server had a screen revealing Microsoft warning message that the software has not been activated – commonly a hallmark of unlicensed "pirated" software. This message can also activate if a substantial part of the server hardware is replaced, causing Windows to consider it to be another computer other than the one the system was licensed for. (Exhibit J)

40. I later watched Dominic shut down all computers other than the server. Yet the network switch in the rack lit to indicate repeating bursts of traffic. Computers which are connected to the Internet frequently transmit data, but I was repeatedly told that the rack network is air gapped. When all computers other than the server were off, and nobody was operating the server, what was causing the traffic bursts is unexplained. It is normal that network switch blinks periodically when server is looking for appliances and other Plug and Play (PnP) devices, but continuous bursts do not fit into that pattern. (Video Exhibit H)

41. When Dominion people realized my interest on the network switch lights, they locked the rack, closing the mesh doors in front of the machines, obscuring visual access.

42. Later Fulton County election official Ralph Jones came to explain that Dominion refused to "give *their* ballots" to us or allow anyone to "use *their* software" to produce records for me for either the test ballots or the June 9 duplicated ballots we had scanned. This statement made no sense to me, because my understanding based on publicly available information is that the county has licensed the software for their use and the voted ballots and images under no circumstances are the property of Dominion.

43. Later I was furnished what was supposed to be the log files for the day's (August 25) activities. A quick look revealed that the logs were not August 25th logs but instead logs of August 11th ending about 5:32pm. After asking for a correction, I realized that, unbeknownst to me, one more Dominion employee had arrived and was troubleshooting in Derrick Gilstrap's office. They again went behind the rack and eventually wrote an USB stick, which was taken out of my view to the office where the additional Dominion employee was working. About 5 minutes later, I was brought USB stick with the August 25th logs.

44. I have been able to start the preliminary analysis of the logs, and the first discovery is that both the August 11th and August 25th logs are incomplete. In the case of the August 25th logs, the logs end at about 12:25pm, shortly after the Dominion employee walked behind the rack and while the activities were still ongoing before adjourning for the lunch. No activities during lunch break were

recorded, while the screens when we returned showed that subsequent activities had taken place

Conclusions from August 25 EPC visit

45. Dominion staff has total control over the server and its logs and therefore the logs are no longer trustworthy. Furthermore, when recent logs were copied for us, they were taken out of view for enough time for a capable person to have ample of time to clean those logs.

46. Fast security log rotation is unacceptable. If there is a secondary storage where the completed logs are stored, those should have been produced to us. Without security logs, it is not possible to determine when remote access software was activated or the activities on the election night.

47. Frequently bursting network traffic when the system was mainly shut down is suspicious and should be investigated.

48. Excuses claiming that the images are not recording, followed by the refusal to load the images is suspicious. If there were no images on the card, a logical action would be to demonstrate that by attempting to load the images to show that there is nothing, instead of claiming that they cannot do so if not ordered by Dominion, even if Fulton County so instructs.

Logic and Accuracy Testing

49. The State Defendants seem to misunderstand the importance of basic functional Logic and Accuracy testing of voting machines. The BMD touchscreens, printers and scanners are all easily hacked and subject to erroneous ballot building and malfunction and should not be deployed into the polling places until each machine has been tested for its ability to accurately register a vote for each candidate in each race and to register an undervote in each contest. The system is far too unreliable to conduct sample counts testing as little as a vote for one candidate for an entire precinct's machines.

50. Although Mr. Chris Harvey said in his declaration (Doc 834-3 ¶¶6-7) that testing all choices on all machines is "overly burdensome and unnecessary because it would require creating and printing" an extremely large test deck. The size of a test deck would rarely be unwieldy, but more importantly, BMDs require testing at minimum level of casting a vote for each position for each race. The cost of such inconvenience and labor expense for standard Logic and Accuracy Testing of BMDs should be factored into the purchase decision, and not shortcut after the fact, furthering diminishing the security of the system.

This 1st day of September, 2020.

Harri Hursti

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRAD RAFFENSPERGER, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF HARRI H. HURSTI

HARRI H. HURSTI declares, under penalty of perjury, pursuant to 28 U.S.C. §1746, that the following is true and correct:

1. My name is Harri H. Hursti.

2. I have personal knowledge of all facts stated in this declaration, and if called to testify, I could and would testify competently thereto.

3. I am a technologist who has worked in security-oriented IT technology for over 30 years and participated in building the first pan-European Internet Service Provider, EUnet. I have extensive knowledge observing, witnessing and preventing malicious activities in networked environments. My background as a cybersecurity expert started in the mid-1980s with technologies to protect

national security level systems, information, and developing secure communication protocols.

4. I have briefed law and policy makers around the world concerning various election security issues, including the Presidential Advisory Commission on Election Integrity on September 12th, 2017.

5. I have briefed state and local governments on election cyber security.

6. I have been researching US election infrastructure security since 2005. The HBO docume.. ary film 'Hacking Democracy' features my successful proof-of-concept mock election hack to alter reported results in an election machine used in US elections.

7. I participated as a researcher when Ohio's Secretary of State commissioned the "Evaluation and Validation of Election-Related Equipment, Standards and Testing", also known as EVEREST. The purpose of the study was to validate all previous research available about voting systems used in Ohio before conducting further research. The report exposed the significant and varied security vulnerabilities in the state's primary voting systems. While this study was published over 10 years ago, it is still relevant, because many system and software versions evaluated then are still widely in use, and the vulnerabilities have not been adequately addressed.

8. I am a co-founder and co-organizer of the DEF CON Voting Machine Hacking Village. The host event, DEF CON, one of the world's largest and most notable global security research and hacker community conventions, is held annually in Las Vegas, Nevada. DEF CON is a 3-day event which attracts about 30,000 attendees.

9. The Voting Machine Hacking Village is an educational event at DEF CON which allows interested parties to research, learn, and study security properties of the voting machines used in the USA and overseas. It is not security testing or evaluation, it is an event where interested parties come to learn and all discoveries are incidental to the main mission, yet new discoveries happen in volumes every year. In 2018, the Voting Machine Hacking Village was awarded a Cybersec. rity Excellence Award. In 2019, we started the "Unhack the Ballot" initiative, aiming to pair local election officials with volunteer hackers to help the officials gain access to security expertise, and better understand the expanse of very real current threats to the nation's election equipment.

10. Every voting machine presented for security research in DEF CON Voting Machine Hacking Village has been hacked during the event. In security research, the participants are only discovering vulnerabilities and reporting

those. Security research does not include the process of weaponization which would include distribution mechanics and deployment. Security research does not aim to produce demonstrable attacks.

11. DEF CON serves as an important looking glass to understand the state of the art in attack development and the emerging new techniques to discover vulnerabilities around the world. An up-to-date understanding of the newest offensive technologies is important for realistic threat analysis and the development of successful defensive and mitigation strategies. The underlying fundamentals of most threats, attack surfaces, and attack vectors are seldom industry-specific. It is very common that the same root causes repeat themselves across a multitude of industries, enabling attackers to target many systems by easy adoption across the board where similar hardware or software designs and architectures are utilized. Voting technology is utilizing a lot of general-purpose hardware and general-purpose operating systems in many parts of the architecture, and therefore it shares a wide range of commonalities in the threat landscape with other seemingly unrelated industries. These commonalities are used by threat actors to move from one target industry to another with greatly lowered barriers.

12. In August 2019, DEF CON introduced two different models of Ballot-Marking Devices for the first time. One of the devices was stand-alone and the other was an integrated ballot marking device with a paper ballot scanner . this kind of machine is sometimes referred to as a 'hybrid' device. Both devices were hacked for the first time within 8 hours of the beginning of the event. The general characteristics of the discoveries underlined the lack of security in both the architecture and the implementation of these systems.

13. Independent security studies like California's Top-to-Bottom Review or EVEREST has not included Ballot-Marking Devices as target systems. Furthermore, many sub-technologies introduced into the voting process with Ballot-Marking Devices, like 2D barcodes, have not been part of the systems tested.

14. These technologies introduce new known and exposed attack surfaces, for example barcodes implementations have been found to introduce new vulnerabilities in studies which are not election system studies, but share relevant similarities in characteristics and architectural elements with election systems. These vulnerabilities spread over multiple source categories of severe vulnerabilities and attack vectors.

15. Academic research and independent studies such as EVEREST and TTBR have not been conducted on barcode generating BMDs as a general class of devices and specifically, Dominion ImageCastX has not been part of the systems studied. However, without studies, just an inspection of publicly available materials like User Manuals reveal many areas of vulnerabilities. Screenshots in the manuals show that the devices have Internet software installed. Furthermore, the sample ballots in the training materials show consistently that the barcode on the ballot does not contain a human-verifiable representation of the .. ter's choices, and that the barcode utilizes the second-lowest error correction setting available in the standard.

16. Based on my background, the current trends in the hacker and security research landscape and the fundamentals shared between the voting infrastructure and elements which have already been compromised and proven to be a source of vulnerabilities, I find it probable that a system like Georgia's Dominion Voting System can and will be targeted by adversarial parties.

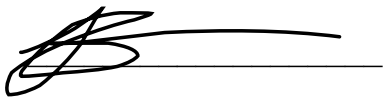
17. Furthermore, considering the available information paired with the threat catalogs at the disposal of the adversaries, it is my professional opinion, a well-funded and motivated adversary can plan and execute a hard-to-detect attack, if not impossible-to-detect the attack against the system. The security community

in general, and election security community specifically considers such attacks as almost inevitable and accepted as such.

18. While the hand marked paper ballot remains the gold standard, Ballot-Marking Devices as computerized systems are subject to cyber-attacks which can compromise the integrity of the paper trail. Without a reliable paper trail, meaningful auditing of the results becomes impossible.

19. A system like Georgia's Dominion V.. ing System has properties which are a target-rich environment for multiple classes of potential threat actors. Based on the documentation available, there are a multitude of exposed attack surfaces for remote and wholesale attacks. Without a thorough security evaluation and analysis of both the system and the deployment plan, the insider attack vectors are harder to enumerate.

Executed on this date, December 16, 2019.



Harri H. Hursti

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,	)	
	)	
Plaintiffs,	)	
	)	**CIVIL ACTION**
vs.	)	
	)	**FILE NO. 1:17-cv-2989-AT**
BRAD RAFFENSPERGER, ET AL.,	)	
	)	
	)	
Defendants.	)	

DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. My background and qualifications in voting system cybersecurity are set forth in my prior declaration, at Document 480-1, pages 37 *et seq.*

3. This statement supplements my declaration of December 16, 2019. I stand by everything in the previous declaration.

4. I am engaged as an expert in this case by Coalition for Good Governance.

5. In developing my declaration and opinion, I visited Atlanta, Georgia, to personally observe certain operations of the June 9, 2020 statewide primary, and the August 11, 2020 runoff. During the June 9 election, I was an authorized poll watcher in some locations and was a public observer in others. On August 11, 2020, I was authorized as an expert inspecting and observing under the Coalition for Good Governance's Rule 34 Inspection activity in certain polling places and the Fulton County Election Preparation Center. I was a public observer in others. As I will explain below in this declaration, my extensive experience in voting system security and my observations in the two mentioned elections lead to my additional conclusions beyond those in my December 16, 2019 that:

a) the electronic pollbooks are based on general purpose consumer grade hardware and operating systems. They are not and cannot be adequately secured against malfunctioning or attacks. They require the standard, universally recommended risk reduction practice of having current paper pollbook backups to be used to issue ballots in the event of emergencies, equipment unreliability, or e-pollbook discrepancies;

b) furthermore, in my processional opinion, backed by "SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION" volumes I-V, electronic pollbook systems present a compelling attack surface for any domestic or foreign adversarial actor who considers disruption or sowing discord as one of the goals and therefore has to always have immediately available backup process;

c) if Georgia's PollPad system has been set to permit unlimited issuance of BMD voter access cards for a single voter, this would constitute a high risk and non-standard election process;

d) the voting system, including its PollPad and BMD related components, is being operated in Fulton County in a manner that escalates the security risk to an extreme level.

Polling Place Observations

6. Election observation on Peachtree Christian Church. My observation at Peachtree Christian Church polling place was authorized by the Rule 34 inspection.

7. The polling location manager explained that he has been instructed to start using the paper backup to check in voters only after power outage which has lasted over 30 minutes.

8. He showed me the paper voter list, that based on the title page, appeared to have been prepared for June 9 primary election. (See Picture at Exhibit A). Marilyn Marks took this picture as she and I inspected the printed voter list.

9. Election observation on Central Park Recreation Center. I observed that the PollPad at one point had to be shut down and restarted at one station in attempt to troubleshoot a wireless networking issue. After restarting, the PollPad required no password from the operator to begin processing voter access smartcards to activate the Ballot Marking Device.

10. Subsequently, I was able to watch the State of Georgia Poll Pad Training Session for the August 11 election. David Greenwalt, Training Administrator for Southeast Elections Director for KnowInk says “One of the things that you’ll notice if you worked in the June election, when we hit the Get

Started Button, we did not have to do the Poll Manager Log In. Um. It was decided after the June election that that was a redundant security measure and so we have excluded the Poll Worker Log In Screen from the process for the August election." at 10:22 -10:44. This video is available at:

https://player.vimeo.com/video/440680300?autoplay=1

11. Permitting operation of electronic pollbooks without password protection is an unacceptable practice from a voting system, or any system processing sensitive data, security standpoint. Federal Information Processing Standards allow no access to sensitive systems with weak passwords, obviously no password is categorically banned.

12. As seen in June in Georgia and across the United States, electronic poll-book systems frequently face issues causing delayed openings of the polling locations and/or long lines. Many times, explanations for electronic poll-book failures have not been investigated, while some studies have found issues in system design. Measures like removing passwords, and therefore weakening the security should never be a workaround to reliability issues.

13. Other states like New Hampshire have added contingency requirements, for example that the electronic poll-book system must be able to

produce an in-location paper backup when needed allowing resuming operation on paper with maximum allowed delay of 15 minutes.

14. Election observation in Central Park Recreation Center. My August 11 observation at Central Park Recreation was authorized by the Coalition's Rule 34 inspection.

15. The Poll place manager told me that no Dominion trained technician had reported on location to help them that morning.

16. Poll workers told me that the electronic poll books were failing to synchronize their check-ins, and therefore they diverted into a manual process to add up the totals from the poll books. When I was present, poll workers started to troubleshoot the issue. Within 10 minutes, they realized that 3 out of 4 poll books were synchronizing and one of the poll books was not connecting to the others while not providing any other indication of that than a yellow warning icon. The pollworkers told me that, until this troubleshooting, which started about 1 hour and 45 minutes after the polls had been opened, the poll workers had assumed that none of the pollbooks synchronized with each other. It is unclear if that was the original situation which had partially self-cured, but with lack of warning messages, the poll workers were apparently missing the changing status of the wireless network.

17. While they were attempting to troubleshoot the issue by rebooting, one of the poll workers realized which poll books had the problem and said that she knew how to access Wi-Fi and Bluetooth setting of the poll books. They managed to reset the connections and connect all poll books around 9 am of the Election Day to working condition.

18. Election observation in Fanplex location. I was at the Fanplex polling place authorized by the Rule 34 inspection. The Fanplex Polling location had accuracy issues with the electronic pollbooks. Voters belonging to a new precinct (0F1) included in the location were not found on the electronic pollbook system. Poll watchers and poll workers reported that once the poll officials followed the telephone instructions of the Elections Office, the voters in 0F1 precinct appeared in the PollPad. However, all voters in the precinct were reportedly displayed as having voted a mail ballot, although voters stated it was inaccurate.

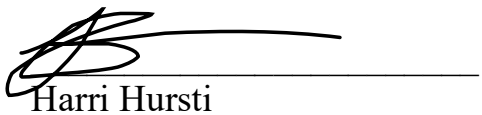
19. It is impossible without an in-depth examination to know the cause of the problem that would cause the voter records to appear in these improper ways. These are prime examples of the need for an updated back up paper pollbook so that such discrepancies can be handled in the polling place permitting voting to continue.

20. Election observation at Park Tavern. I was at Park Tavern polling place authorized by the Rule 34 inspection. Poll workers operating electronic pollbooks explained that during this election they were not connected into the Internet like they were in the previous election. They stated that they are using local area wireless networking.

Conclusions

21. The current implementation of electronic pollbooks is not stable and caused delayed openings of the polling locations and long lines. To try and correct this instability, passwords were removed, but removing the passwords makes them a vulnerable, high risk high reward attack target for an adversary of any skill level who either seeks publicity or is deliberately disenfranchising targeted voters. Passwords must be required. In addition, it is imperative that up-to-date paper pollbook backups to be used to issue ballots in the event of emergencies, equipment unreliability, or e-pollbook discrepancies.

Executed this 21st day of August 2020.



Harri Hursti

EXHIBIT

2

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,	)	
	)	
Plaintiffs,	)	
	)	**CIVIL ACTION**
vs.	)	
	)	**FILE NO. 1:17-cv-2989-AT**
BRAD RAFFENSPERGER, ET AL.,	)	
	)	
Defendants.	)	

DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. My background and qualifications in voting system cybersecurity are set forth in my December 16, 2019 declaration. (Doc. 680-1, pages 37 *et seq*). I stand by everything in that declaration and in my August 21, 2020 declaration. (Doc. 800-2).

3. I am also an expert in ballot scanning because of extensive background in digital imaging prior by work researching election systems. In addition, in 2005 I started an open source project for scanning and auditing paper ballots from images. As a result, I am familiar with different scanner types, how scanner settings and image processing features change the images, and how file format choices affect the quality and accuracy of the ballots.

4. I am engaged as an expert in this case by Coalition for Good Governance.

5. In developing this declaration and opinion, I visited Atlanta to observe certain operations of the June 9, 2020 statewide primary, and the August 11 runoff. During the June 9 election, I was an authorized poll watcher in some locations and was a public observer in others. On August 11, I was authorized as an expert inspecting and observing under the Coalition for Good Governance's Rule 34 Inspection request in certain polling places and the Fulton County Election Preparation Center. As I will explain below in this declaration, my extensive experience in the area of voting system security and my observations of these elections lead to additional conclusions beyond those in my December 16, 2019 declaration. Specifically:

a) the scanner and tabulation software settings being employed to determine which votes to count on hand marked paper ballots are likely causing clearly intentioned votes not to be counted;

b) the voting system is being operated in Fulton County in a manner that escalates the security risk to an extreme level; and

c) voters are not reviewing their BMD printed ballots, which causes BMD generated results to be un-auditable due to the untrustworthy audit trail.

Polling Place Observations

6. Election observation on Peachtree Christian Church. The ballot marking devices were installed so that 4 out of 8 touchscreen devices were clearly visible from the pollbook check in desk. Voter's selections could be effortlessly seen from over 50 ft away.

7. Over period of about 45 minutes, I only observed one voter who appeared to be studying the ballot after picking it up from the printer before casting it in the scanner. When voters do not fully verify their ballot prior to casting, the ballots cannot be considered a reliable auditable record.

8. The scanner would reject some ballots and then accept them after they were rotated to a different orientation. I noted that the scanner would vary in the amount of time that it took to accept or reject a ballot. The delay varied between 3

and 5 seconds from the moment the scanner takes the ballot until the scanner either accepts the ballot or rejects it. This kind of behavior is normal on general purpose operating systems multitasking between multiple applications, but a voting system component should be running only a single application without outside dependencies causing variable execution times.

9. Further research is necessary to determine the cause of the unexpected scanning delays. A system that is dedicated to performing one task repeatedly should not have unexplained variation in processing time. As security researcher, we are always suspicious about any unexpected variable delays, as those are common telltale signs of many issues, including a possibility of unauthorized code being executed. So, in my opinion changes of behaviors between supposedly identical machines performing identical tasks should always be investigated.

When ballots are the same and are produced by a ballot marking device, there should be no time difference whatsoever in processing the bar codes. Variations in time can be the result of many things - one of them is that the scanner encounters an error reading the bar code and needs to utilize error correcting algorithms to recover from that error. Further investigation is

necessary to determine the root cause of these delays, the potential impact of the error correcting algorithms if those are found to be the cause, and whether the delay has any impact upon the vote.

10. Election observation in Central Park Recreation Center. The Poll place manager told me that no Dominion trained technician had reported on location to help them that morning.

11. The ballot marking devices were originally installed in a way that voter privacy was not protected, as anyone could observe across the room how people are voting on about 2/3 devices.

12. The ballot scanner took between 4 and 6 seconds to accept the ballot. I observed only one ballot being rejected.

13. Generally, voters did not inspect the ballots after taking it from the printer and casting it into the scanner.

14. Election observation in Fanplex location. Samantha Whitley and Harrison Thweatt were poll watchers at the Fanplex polling location. They contacted me at approximately 9:10am about problems they were observing with the operation of the BMDs and Poll Pads and asked me to come to help them

understand the anomalies they were observing. I arrived at FanPlex at approximately 9:30am.

15. I observed that the ballot scanner located by a glass wall whereby standing outside of the building observe the scanning, would take between 6 and 7 seconds to either accept or reject the ballot.

16. For reasons unknown, on multiple machines, while voters were attempting to vote, the ballot marking devices sometimes printed "test" ballots. I was not able to take a picture of the ballot from the designated observation area, but I overheard the poll worker by the scanner explaining the issue to a voter which was sent back to the Ballot-Marking Device to pick up another ballot from the printer tray. Test ballots are intended to be used to test the system but without being counted by the system during an election. The ballot scanner in election settings rejects test ballots, as the scanners at FanPlex did. This caused confusion as the voters needed to return to the ballot-marking device to retrieve the actual ballot. Some voters returned the test ballot into the printer tray, potentially confusing the next voter. Had voters been reviewing the ballots at all before taking them to the scanner, they would have noticed the "Test Ballot" text on the ballot. I observed no voter really questioning a poll worker why a "Test" ballot was printed in the first place.

17. Obviously, during the election day, the ballot marking device should not be processing or printing any ballot other than the one the voter is voting. While the cause of the improper printing of ballots should be examined, the fact that this was happening at all is likely indicative of a wrong configuration given to the BMD, which in my professional opinion raises another question: Why didn't the device print only test ballots? And how can the device change its behavior in the middle of the election day? Is the incorrect configuration originating from the Electronic Pollbook System? What are the implications for the reliability of the printed ballot and the QR code being counted?

18. Election observation Park Tavern. The scanner acceptance delay did not vary as it had in previous locations and was consistently about 5 seconds from the moment the scanner takes the ballot, to the moment the scanner either accepts the ballot or rejects it. The variation between scanners at different locations is concerning because these are identical physical devices and should not behave differently while performing the identical task of scanning a ballot.

19. The vast majority of voters at Park Tavern did not inspect the ballots after taking them from the printer and before casting them in the scanner.

Fulton Tabulation Center Operation-Election Night, August 11, 2020

20. In Fulton County Election Preparation Center ("EPC") on election night I reviewed certain operations as authorized by Rule 34 inspection.

21. I was permitted to view the operations of the upload of the memory devices coming in from the precincts to the Dominion Election Management System ("EMS") server. The agreement with Fulton County was that I could review only for a limited period of time; therefore, I did not review the entire evening's process. Also, Dominion employees asked me to move away from the monitors containing the information and messages from the upload process and error messages, limiting my ability to give a more detailed report with documentation and photographs of the screens. However, my vantage point was more than adequate to observe that system problems were recurring and the Dominion technicians operating the system were struggling with the upload process.

22. It is my understanding the same EMS equipment and software had been used in Fulton County's June 9, 2020 primary election.

23. It is my understanding that the Dominion technician ("Dominic") charged with operating the EMS server for Fulton County had been performing

these duties at Fulton County for several months, including during the June 9 primary.

24. During my August 11 visit, and a follow-up visit on August 17, I observed that the EMS server was operated almost exclusively by Dominion personnel, with little interaction with EPC management, even when problems were encountered. In my conversations with Derrick Gilstrap and other Fulton County Elections Department EPC personnel, they professed to have limited knowledge of or control over the EMS server and its operations.

25. Outsourcing the operation of the voting system components directly to the voting system vendors' personnel is highly unusual in my experience and of grave concern from a security and conflict of interest perspective. Voting system vendors' personnel have a conflict of interest because they are not inclined to report on, or address, defects in the voting systems. The dangers this poses is aggravated by the absence of any trained County personnel to oversee and supervise the process.

26. In my professional opinion, the role played by Dominion personnel in Fulton County, and other counties with similar arrangements, should be considered an elevated risk factor when evaluating the security risks of Georgia's voting system.

27. Based on my observations on August 11 and August 17, Dell computers running the EMS that is used to process Fulton county votes appeared not to have been hardened.

28. In essence, hardening is the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle it is to the reduce the general purpose system into a single-function system which is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, grant accounts and programs with the minimum level of privileges needed for the tasks and create separate accounts for privileged operations as needed, and the disabling or removal of unnecessary services.

29. Computers performing any sensitive and mission critical tasks such as elections should unquestionably be hardened. Voting system are designated by the Department of Homeland Security as part of the critical infrastructure and certainly fall into the category of devices which should be hardened as the most fundamental security measure. In my experience, it is unusual, and I find it unacceptable for an EMS server not to have been hardened prior to installation.

30. The Operating System version in the Dominion Election Management computer, which is positioned into the rack and by usage pattern appears to be the main computer, is Windows 10 Pro 10.0.14393. This version is also known as the Anniversary Update version 1607 and it was released August 2, 2016. Exhibit A is a true and correct copy of a photograph that I took of this computer.

31. When a voting system is certified by the EAC, the Operating System is specifically defined, as Windows 10 Pro was for the Dominion 5.5-A system. Unlike consumer computers, voting systems do not and should not receive automatic "upgrades" to newer versions of the Operating System. without undergoing tests for conflicts with the new operating system software.

32. That computer and other computers used in Georgia's system for vote processing appear to have home/small business companion software packages included. Exhibits B and C are true and correct copies of photographs that I took of the computer located in the rack and the computer located closest to the rack on the table to the right. The Start Menu shows a large number of game and entertainment software icons. As stated before, one of the first procedures of hardening is removal of all unwanted software, and removal of those game icons and the associated games and installers alongside with all other software which is not absolutely needed in the computer for election processing purposes would be

one of the first and most basic steps in the hardening process. In my professional opinion, independent inquiry should be promptly made of all 159 counties to determine if the Dominion systems statewide share this major deficiency.

33. Furthermore, when I asked the Dominion employee Dominic assigned to the Fulton County election server operation about the origin of the Windows operating system, he answered that he believed that "it has been provided by the State."

34. Since Georgia's Dominion system is new, it is a reasonable assumption that all machines in the Fulton County election network had the same version of Windows installed. However, not only the two computers displayed different entertainment software icons, but additionally one of the machines in Fulton's group of election servers had an icon of computer game called "*Homescapes"* which is made by Playrix Holding Ltd., founded by Dmitry and Igor Bukham in Vologda, Russia. Attached as Exhibit C is a true and correct copy of a photograph that I took of the Fulton voting system computer" Client 02". The icon for Homescapes is shown by the arrow on Exhibit C.

35. The *Homescapes* game was released in August 2017, one year after Fulton County's operating system release. If the *Homescapes* game came with the operating system it would be unusual, because at the time of the release of

Homescapes, Microsoft had already released 3 major Microsoft Windows 10 update releases after build 14393 and before the release of that game. This calls into question whether all Georgia Dominion system computers have the same operating system version, or how the game has come to be having a presence in Fulton's Dominion voting system.

36. Although this Dominion voting system is new to Georgia, the Windows 10 operating system of at least the 'main' computer in the rack has not been updated for 4 years and carries a wide range of well-known and publicly disclosed vulnerabilities. At the time of this writing, The National Vulnerability Database maintained by National Institute of Standards and Technology lists 3,177 vulnerabilities mentioning "Windows 10 Pro" and 203 vulnerabilities are specifically mentioning "Windows 10 Pro 1607" which is the specific version number of the build 14393 that Dominion uses.

37. Even without internet connectivity, unhardened computers are at risk when those are used to process removable media. It was clear that when Compact Flash storage media containing the ballot images, audit logs and results from the precinct scanners were connected to the server, the media was automounted by the operating system. When the operating system is automounting a storage media, the operating system starts automatically to interact with the device. The zero-day

vulnerabilities exploiting this process has been recurringly discovered from all operating systems, including Windows. Presence of automount calls also into question presence of another setting which is always disabled in hardening process. It is autorun, which automatically executes some content on the removable media. While this is convenient for consumers, it poses extreme security risk.

38. Based on my experience and mental impression observing the Dominion technician's activities, Fulton County's EMS server management seems to be an *ad hoc* operation with no formalized process. This was especially clear on the manual processing of the memory cards storage devices coming in from the precincts on election night and the repeated access of the operating system to directly access filesystem, format USB devices, etc. This kind of operation in naturally prone to human errors. I observed personnel calling on the floor asking if all vote carrying compact flash cards had been delivered from the early voting machines for processing, followed by later finding additional cards which had been overlooked in apparent human error. Later, I heard again one technician calling on the floor asking if all vote carrying compact flashes had been delivered. This clearly demonstrates lack of inventory management which should be in place to ensure, among other things, that no rogue storage devices would be inserted into the computer. In response, 3 more compact flash cards were hand-delivered. Less

than 5 minutes later, I heard one of the county workers say that additional card was found and was delivered for processing. All these devices were trusted by printed label only and no comparison to an inventory list of any kind was performed.

39. In addition, operations were repeatedly performed directly on the operating system. Election software has no visibility into the operations performed directly on the operating system, and therefore those are not included in election system event logging. Those activities can only be partially reconstructed from operating system logs – and as these activities included copying election data files, election software log may create false impression that the software is accessing the same file over a period of time, while in reality the file could had been replaced with another file with the same name by activities commanded to the operating system. Therefore, any attempt to audit the election system operated in this manner must include through analysis of all operating system logs, which complicates the auditing process. Unless the system is configured properly to collect file system auditing data is not complete. As the system appears not to be hardened, it is unlikely that the operating system has been configured to collect auditing data.

40. A human error when operating live election system from the operating system can result in a catastrophic event destroying election data or even rendering the system unusable. Human error is likely given the time pressure involved and,

at least in Fulton County, no formal check lists or operating procedures were followed to mitigate the human error risk. The best practice is to automate trivial tasks to reduce risk of human error, increase the quality assurance of overall operations and provide auditability and transparency by logging.

41. Uploading of memory cards had already started before I arrived at EPC. While one person was operating the upload process, the two other Dominion employees were troubleshooting issues which seemed to be related to ballot images uploads. I repeatedly observed error messages appearing on the screen of the EMS server. I was not able to get picture of the errors on August 11th, I believe the error was the same or similar that errors recurring August 17th as shown on Exhibit D and discussed later in this declaration. Dominion employees were troubleshooting the issue with 'trial-and-error' approach. As part of this effort they accessed "Computer Management" application of Windows 10 and experimented with trouble shooting the user account management feature. This demonstrates that they had complete access to the computer. This means there are no meaningful access separation and privileges and roles controls protecting the county's primary election servers. This also greatly amplifies the risk of catastrophic human error and malicious program execution.

42. I overheard the Dominion technician's conversation that they had issues with file system structure and "need 5 files out of EMS server and paste. Delete everything out of there and put it there." To communicate the gravity of the situation to each other they added "Troubleshooting in the live environment". These conversations increased the mental image that they were not familiar the issue they were troubleshooting.

43. After about 45 minutes of trying to solve the issue by instructions received over the phone, the two Dominion employees' (who had been troubleshooting) behavior changed. The Dominion staff member walked behind the server rack and made manual manipulations which could not be observed from my vantage point. After that they moved with their personal laptops to a table physically farther away from the election system and stopped trying different ways to work around the issue in front of the server, and no longer talked continuously with their remote help over phone.

44. In the follow-up-calls I overheard them ask people on the other end of the call to check different things, and they only went to a computer and appeared to test something and subsequently take a picture of the computer screen with a mobile phone and apparently send it to a remote location.

45. Based on my extensive experience, this all created a strong mental impression that the troubleshooting effort was being done remotely over remote access to key parts of the system. Additionally, new wireless access point with a hidden SSID access point name appeared in the active Wi-Fi stations list that I was monitoring, but it may have been co-incidental. Hidden SSIDs are used to obscure presence of wireless networking from casual observers, although they do not provide any real additional security.

46. If in fact remote access was arranged and granted to the server, this has gravely serious implications for the security of the new Dominion system. Remote access, regardless how it is protected and organized is always a security risk, but furthermore it is transfer of control out of the physical perimeters and deny any ability to observe the activities.

47. I also observed USB drives marked with the Centon DataStick Pro Logo with no visible inventory control numbering system being taken repeatedly from the EMS server rack to the Fulton managers' offices and back. The Dominion employee told me that the USB drives were being taken to the Election Night Reporting Computer in another office. This action was repeated several times during the time of my observation. Carrying generic unmarked and therefore unidentifiable media out-of-view and back is a security risk – especially when the

exact same type of devices was piled on the desk near the computer. During the election night, the Dominion employees reached to storage box and introduced more unmarked storage devices into the ongoing election process. I saw no effort made to maintain a memory card inventory control document or chain of custody accounting for memory cards from the precincts.

48. I also visited the EPC on August 17. During that visit, the staff working on uploading ballots for adjudication experienced an error which appeared similar to the one on election night. This error was repeated with multitude of ballots and at the time we left the location, the error appeared to be ignored, rather that resolved. (EXHIBIT D - the error message and partial explanation of the error being read by the operator.).

49. The security risks outlined above – operating system risks, the failure to harden the computers, performing operations directly on the operating systems, lax control of memory cards, lack of procedures, and potential remote access, are extreme and destroy the credibility of the tabulations and output of the reports coming from a voting system.

50. Such a risk could be overcome if the election were conducted using hand marked paper ballots, with proper chain of custody controls. For elections conducted with hand marked paper ballots, any malware or human error involved

in the server security deficiencies or malfunctions could be overcome with a robust audit of the hand marked paper ballots and in case of irregularities detected, remedied by a recount. However, given that BMD ballots are computer marked, and the ballots therefore unauditable for determining the result, no recovery from system security lapses is possible for providing any confidence in the reported outcomes.

Ballot Scanning and Tabulation of Vote Marks

51. I have been asked to evaluate the performance and reliability of Georgia's Dominion precinct and central count scanners in the counting of votes on hand marked paper ballots.

52. On or about June 10th, Jeanne Dufort and Marilyn Marks called me to seek my perspective on what Ms. Dufort said she observed while serving as a Vote Review Panel member in Morgan County. Ms. Dufort told me that she observed votes that were not counted as votes nor flagged by the Dominion adjudication software.

53. Because of the ongoing questions this raised related to the reliability of the Dominion system tabulation of hand marked ballots, I was asked by Coalition Plaintiffs to conduct technical analysis of the scanner and tabulation accuracy. That analysis is still in its early stages.

54. Before addressing the particulars of my findings and research into the accuracy of Dominion's scanning and tabulation, I will address the basic process by which an image on a voted hand marked paper ballot is processed by scanner and tabulation software generally. It is important to understand that the Dominion scanners are Canon off the shelf scanners and their embedded software were designed for different applications than ballot scanning which is best conducted with scanners specifically designed for detecting hand markings on paper ballots.

55. Contrary of public belief, the scanner is not taking a picture of the paper. The scanner is illuminating the paper with a number of narrow spectrum color lights, typically 3, and then using software to produce an approximation what the human eye would be likely to see if there would had been a single white wide-spectrum light source. This process takes place in partially within the scanner and embedded software in the (commercial off the shelf) scanner and partially in the driver software in the host computer. It is guided by number of settings and configurations, some of which are stored in the scanner and some in the driver software. The scanner sensors gather more information than will be saved into the resulting file and another set of settings and configurations are used to drive that part of the process. The scanners also produce anomalies which are automatically removed from the images by the software. All these activities are performed

outside of the Dominion election software, which is relying on the end product of this process as the input.

56. I began reviewing Dominion user manuals in the public domain to further investigate the Dominion process.

57. On August 14, I received 2 sample Fulton County August 11 ballots of high-speed scanned ballot from Rhonda Martin, who stated that she obtained them from Fulton County during Coalition Plaintiff's discovery. The image characteristics matched the file details I had seen on the screen in EPC. The image is TIFF format, about 1700 by 2200 pixels with 1-bit color depth (= strictly black or white pixels only) with 200 by 200 dots per square inch ("dpi") resolution resulting in files that are typically about 64 or 73 kilo bytes in size for August 11 ballots. With this resolution, the outer dimension of the oval voting target is about 30 by 25 pixels. The oval itself (that is, the oval line that encircles the voting target) is about 2 pixels wide. The target area is about 450 pixels; the area of the target a tight bounding box would be 750 pixels and the oval line encircling the target is 165 pixels. In these images, the oval itself represented about 22% value in the bounding box around the vote target oval.

58. Important image processing decisions are done in scanner software and before election software threshold values are applied to the image. These

scanner settings are discussed in an excerpt Dominion's manual for ICC operations My understanding is that the excerpt of the Manual was received from Marilyn Marks who stated that she obtained it from a Georgia election official in response to an Open Records request. Attached as Exhibit E is page 9 of the manual. Box number 2 on Exhibit E shows that the settings used are not neutral factory default settings.

59. Each pixel of the voters' marks on a hand marked paper ballot will be either in color or gray when the scanner originally measures the markings. The scanner settings affect how image processing turns each pixel from color or gray to either black or white in the image the voting software will later process. This processing step is responsible for major image manipulation and information reduction before the election software threshold values are calculated. This process has a high risk of having an impact upon how a voter mark is interpreted by the tabulation software when the information reduction erases markings from the scanned image before the election software processes it.

60. In my professional opinion, any decision by Georgia's election officials about adopting or changing election software threshold values is premature before the scanner settings are thoroughly tested, optimized and locked.

61. The impact of the scanner settings is minimal for markings made with a black felt pen but can be great for markings made with any color ballpoint pens. To illustrate this, I have used standard color scanning settings and applied then standard conversion from a scanned ballot vote target with widely used free and open source image processing software "GNU Image Manipulation Program version 2.10.18" EXHIBIT G shows the color image being converted with the software's default settings from color image to Black-and-White only. The red color does not meet the internal conversion algorithm criteria for black, therefore it gets erased to white instead.

62. Dominion manual for ICC operations clearly show that the scanner settings are changed from neutral factory default settings. EXHIBIT H shows how these settings applied different ways alter how a blue marking is converted into Black-and-White only image.

63. The optimal scanner settings are different for each model of scanner and each type of paper used to print ballots. Furthermore, because scanners are inherently different, the manufacturers use hidden settings and algorithms to cause neutral factory settings to produce similar baseline results across different makes and models. This is well-studied topic; academic and image processing studies published as early as 1979 discuss the brittleness of black-or-white images in

conversion. Subsequently, significance for ballot counting has been discussed in academic USENIX conference peer-reviewed papers.

64. On the August 17th at Fulton County Election Preparation Center Professor Richard DeMillo and I participated in a scan test of August 11 test ballots using a Fulton County owned Dominion precinct scanner. Two different ballot styles were tested, one with 4 races and one with 5 races. Attached as Exhibits I and J show a sample ballots with test marks.

65. A batch of 50 test ballots had been marked by Rhonda Martin with varying types of marks and varying types of writing instruments that a voter might use at home to mark an absentee ballot. Professor DeMillo and I participated in marking a handful of ballots.

66. Everything said here concerning the August 17 test is based on a very preliminary analysis. The scanner took about 6 seconds to reject the ballots, and one ballot was only acceptable "headfirst" while another ballot only "tail first." Ballot scanners are designed to read ballots "headfirst" or "tail first," and front side and backside and therefore there should not be ballots which are accepted only in one orientation. I observed the ballots to make sure that both ballots had been cleanly separated from the stub and I could not identify any defects of any kind on the ballots.

67. There was a 15 second cycle from the time the precinct scanner accepted a ballot to the time it was ready for the next ballot. Therefore, the maximum theoretical capacity with the simple 5 race ballot is about 4 ballots per minute if the next ballot is ready to be fed into the scanner as soon as the scanner was ready to take it. In a real-world voting environment, it takes considerably longer because voters move away from the scanner, the next voter must move in and subsequently figure where to insert the ballot. The Dominion precinct scanner that I observed was considerably slower than the ballot scanners I have tested over the last 15 years. This was done with a simple ballot, and we did not test how increase of the number of races or vote targets on the ballot would affect the scanning speed and performance.

68. Though my analysis is preliminary, this test reveals that a significant percentage of filled ovals that would to a human clearly show voter's intent failed to register as a vote on the precinct count scanner.

69. The necessary testing effort has barely begun at the time of this writing, as only limited access to equipment has been made available. I have not had access to the high-volume mail ballot scanner that is expected to process millions of mail ballots in Georgia's upcoming elections. However, initial results suggest that significant revisions must be made in the scanning settings to avoid a

widespread failure to count certain valid votes that are not marked as filled in ovals. Without testing, it is impossible to know, if setting changes alone are sufficient to cure the issue.

Scanned Ballot Tabulation Software Threshold Settings

70. Georgia is employing a Dominion tabulation software tool called "Dual Threshold Technology" for "marginal marks." (See Exhibit M) The intent of the tool is to detect voter marks that could be misinterpreted by the software and flag them for review. While the goal is admirable, the method of achieving this goal is quite flawed.

71. While it is compelling from development cost point of view to use commercial off the shelf COTS scanners and software, it requires additional steps to ensure that the integration of the information flow is flawless. In this case, the software provided by the scanner manufacturer and with settings and configurations have great impact in how the images are created and what information is removed from the images before the election software processes it. In recent years, many defective scanner software packages have been found. These software flaws include 'image enhancement' features which have remained enabled even when the feature has been chosen to be disabled from the scanner software provided by the manufacturer. An example of dangerous feature to keep

enabled is 'Punch Hole Removal', intended to make images of documents removed from notebook binders to look more aesthetically pleasing. The software can and in many cases will misinterpret a voted oval as a punch hole and erase the vote from the image file and to make this worse, the punch holes are expected to be found only in certain places near the edge of the paper, and therefore it will erase only votes from candidates whose targets are in those target zones.

72. Decades ago, when computing and storage capacity were expensive black-and-white image commonly meant 1-bit black-or-white pixel images like used by Dominion system. As computer got faster and storage space cheaper during the last 2-3 decades black-and-white image has become by default meaning 255 shades of gray grayscale images. For the purposes of reliable digitalization of physical documents, grayscale image carries more information from the original document for reliable processing and especially when colored markings are being processed. With today's technology, the difference in processing time and storage prices between grayscale and 1-bit images has become completely meaningless, and the benefits gained in accuracy are undeniable.

73. I am aware that the Georgia Secretary of State's office has stated that Georgia threshold settings are national industry standards for ballot scanners (Exhibit K). This is simply untrue. If, there were an industry standard for that, it

would be part of EAC certification. There is no EAC standard for such threshold settings. As mentioned before, the optimal settings are products of many elements. The type of the scanner used, the scanner settings and configuration, the type of the paper used, the type of the ink printer has used in printing the ballots, color dropout settings, just to name few. Older scanner models, which were optical mark recognitions scanners, used to be calibrated using calibration sheet – similar process is needed to be established for digital imaging scanners used this way as the ballot scanners.

74. Furthermore, the software settings in Exhibit E box 2 show that the software is instructed to ignore all markings in red color ("Color drop-out: Red"), This clearly indicates that the software was expecting the oval to be printed in Red and therefore it will be automatically removed from the calculation. The software does not anticipate printed black ovals as used in Fulton County. Voters have likely not been properly warned that any pen they use which ink contains high concentration of red pigment particles is at risk of not counting, even if to the human eye the ink looks very dark.

75. I listened to the August 10 meeting of the State Board of Elections as they approved a draft rule related to what constitutes a vote, incorporating the following language:

> *Ballot scanners that are used to tabulate optical scan ballots marked by hand shall be set so that:*
>
> *1. Detection of 20% or more fill-in of the target area surrounded by the oval shall be considered a vote for the selection;*
>
> *2. Detection of less than 10% fill-in of the target area surrounded by the oval shall not be considered a vote for that selection;*
>
> *3. Detection of at least 10% but less than 20% fill-in of the target area surrounded by the oval shall flag the ballot for adjudication by a vote review panel as set forth in O.C.G.A. 21-2-483(g). In reviewing any ballot flagged for adjudication, the votes shall be counted if, in the opinion of the vote review panel, the voter has clearly and without question indicated the candidate or candidates and answers to questions for which such voter desires to vote.*

76. The settings discussed in the rule are completely subject to the scanner settings. How the physical marking is translated into the digital image is determined by those values and therefore setting the threshold values without at the same time setting the scanner settings carries no value or meaning. If the ballots will be continuing to be printed with black only, there is no logic in having any drop-out colors.

77. Before the State sets threshold standards for the Dominion system, extensive testing is needed to establish optimal configuration and settings for each step of the process. Also, the scanners are likely to have settings additional configuration and settings which are not visible menus shown in the manual excerpt. All those should be evaluated and tested for all types of scanners approved for use in Georgia, including the precinct scanners

78. As temporary solution, after initial testing, the scanner settings and configuration should be locked and then a low threshold values should be chosen. All drop-out colors should be disabled. This will increase the number of ballots chosen for human review and reduce the number of valid votes not being counted as cast.

Logic and Accuracy Testing

79. Ballot-Marking Device systems inherits the same well-documented systemic security issues embedded in direct-recording electronic (DRE) voting machine design. Such design flaws eventually are causing the demise of DRE voting system across the country as it did in Georgia. In essence the Ballot Marking Device is a general-purpose computer running a general-purpose operating system with touchscreen that is utilized as a platform to run a software, very similar to DRE by displaying a ballot to the voter and recording the voter's intents. The main difference is that instead of recording those internally digitally, it prints out a ballot summary card of voter's choices.

80. Security properties of this approach would be positively different from DREs if the ballot contained only human-readable information and all voters are required to and were capable of verifying their choices from the paper ballot summary. That of course is unrealistic.

81. When voter fails to inspect the paper ballot and significant portion of the information is not in human readable from as a QR barcode, Ballot-Marking Device based voting effectively inherits most of the negative and undesirable security and reliability properties directly from DRE paradigm, and therefore should be subject to the same testing requirements and mitigation strategies as DREs.

82. In response to repeating myriad of issues with DREs, which have been attributed to causes from screen calibration issues to failures in ballot definition configuration distribution, a robust Logic & Accuracy testing regulation have been established. These root causes are present in BMDs and therefore should be evaluated in the same way as DREs have been.

I received the Georgia Secretary of State's manual "Logic and Accuracy Procedures "Version 1.0 January 2020 from Rhonda Martin. Procedure described in section D "Testing the BMD and Printer" is taking significant shortcuts, presumably to cut the labor work required. (Section D is attached as Exhibit L) These shortcuts significantly weaken the security and reliability posture of the system and protections against already known systemic pitfalls, usability predicaments and security inadequacies.

CONCLUSIONS

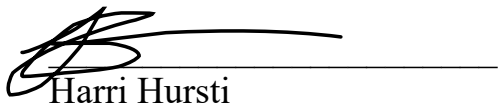
83. The scanner software and tabulation software settings and configurations being employed to determine which votes to count on hand marked paper ballots are likely causing clearly intentioned votes not to be counted as cast.

84. The method of using 1-bit images and calculated relative darkness values from such pre-reduced information to determine voter marks on ballots is severely outdated and obsolete. It artificially and unnecessarily increases the failure rates to recognize votes on hand-marked paper ballots. As a temporary mitigation, optimal configurations and settings for all steps of the process should be established after robust independent testing to mitigate the design flaw and augment it with human assisted processes, but that will not cure the root cause of the software deficiency which needs to be addressed.

85. The voting system is being deployed, configured and operated in Fulton County in a manner that escalates the security risk to an extreme level and calls into question the accuracy of the election results. The lack of well-defined process and compliance testing should be addressed immediately using independent experts. The use and the supervision of the Dominion personnel operating Fulton County's Dominion Voting System should be evaluated.

86. Voters are not reviewing their BMD printed ballots before scanning and casting them, which causes BMD-generated results to be un-auditable due to the untrustworthy audit trail. Furthermore, because BMDs are inheriting known fundamental architectural deficiencies from DREs, no mitigation and assurance measures can be weakened, including but not limited to Logic and Accuracy Testing procedures.

This 24th day of August 2020.



Harri Hursti

EXHIBIT A:

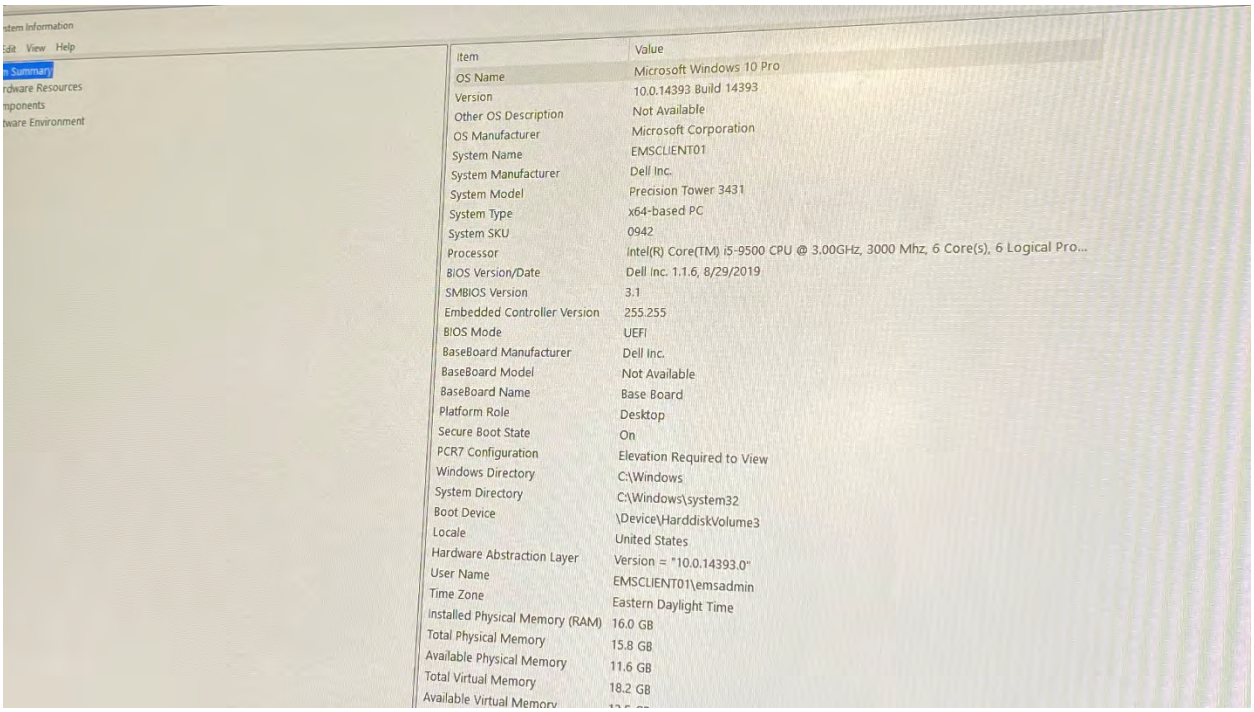

stem Information
Edit View Help
Summary
rdware Resources
mponents
tware Environment
Item
Value
OS Name
Microsoft Windows 10 Pro
Version
10.0.14393 Build 14393
Other OS Description
Not Available
OS Manufacturer
Microsoft Corporation
System Name
EMSCLIENT01
System Manufacturer
Dell Inc.
System Model
Precision Tower 3431
System Type
x64-based PC
System SKU
0942
Processor
Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, 3000 Mhz, 6 Core(s), 6 Logical Pro...
BIOS Version/Date
Dell Inc. 1.1.6, 8/29/2019
SMBIOS Version
3.1
Embedded Controller Version
255.255
BIOS Mode
UEFI
BaseBoard Manufacturer
Dell Inc.
BaseBoard Model
Not Available
BaseBoard Name
Base Board
Platform Role
Desktop
Secure Boot State
On
PCR7 Configuration
Elevation Required to View
Windows Directory
C:\Windows
System Directory
C:\Windows\system32
Boot Device
\Device\HarddiskVolume3
Locale
United States
Hardware Abstraction Layer
Version = "10.0.14393.0"
User Name
EMSCLIENT01\emsadmin
Time Zone
Eastern Daylight Time
Installed Physical Memory (RAM)
16.0 GB
Total Physical Memory
15.8 GB
Available Physical Memory
11.6 GB
Total Virtual Memory
18.2 GB
Available Virtual Memory

EXHIBIT B:


Most used
EMS Election Event Designer
File Explorer
EMS Results Tally and Reporting
Notepad
ImageCast® Adjudication
Calculator
1-Wire Drivers x64
3D Builder
Acrobat Reader DC
Alarms & Clock
Calculator
Calendar
Camera
Life at a glance
Monday
17
Get all your mail in one place
Mail
Microsoft Edge
Photos
Weather
Skype Preview
Microsoft News
Store
Play and explore
Xbox
Groove Music
Movies & TV
Paint 3D
WinZip Univer...
Get Office
OneNote

EXHIBIT C:

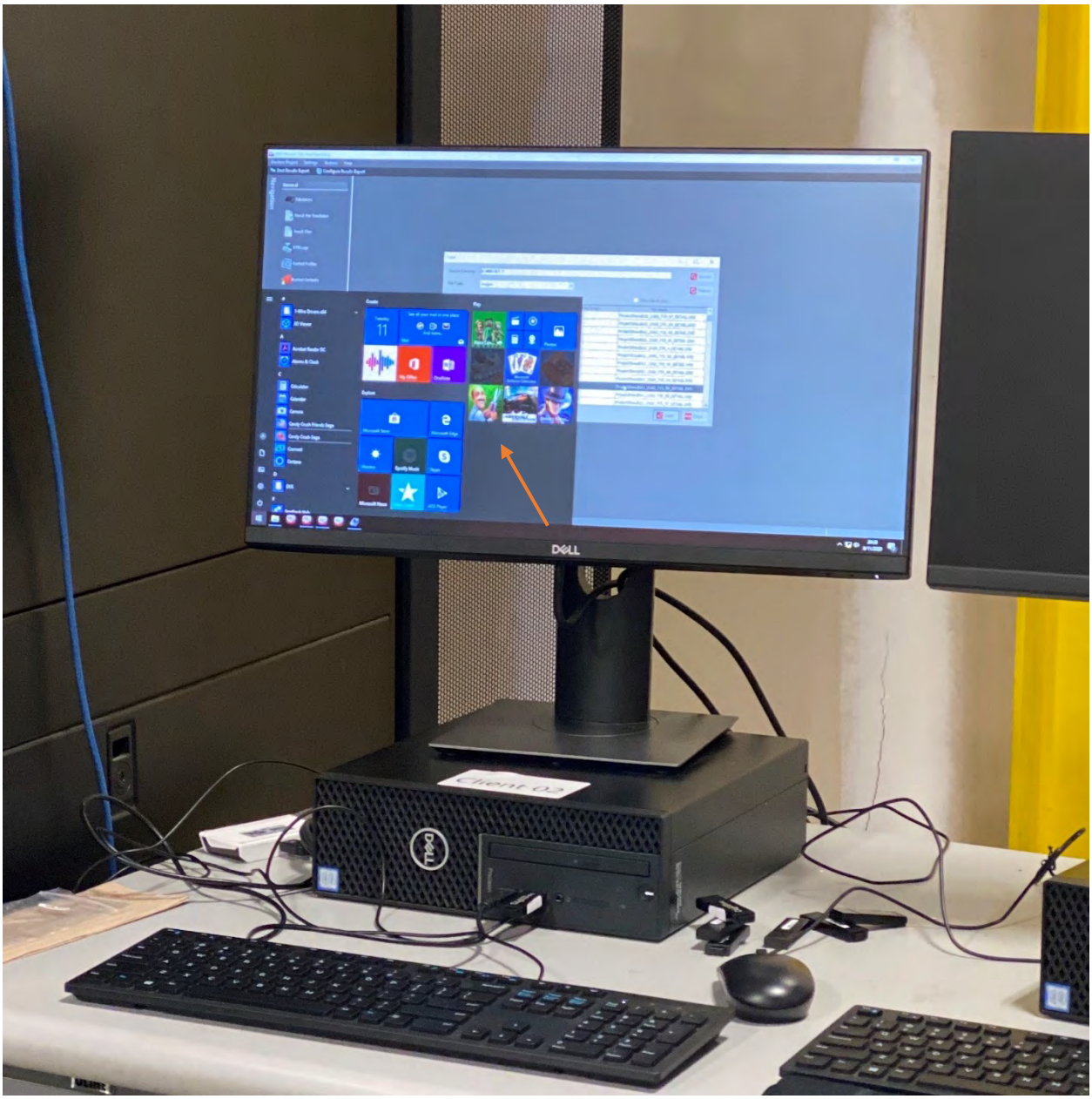


EXHIBIT D:

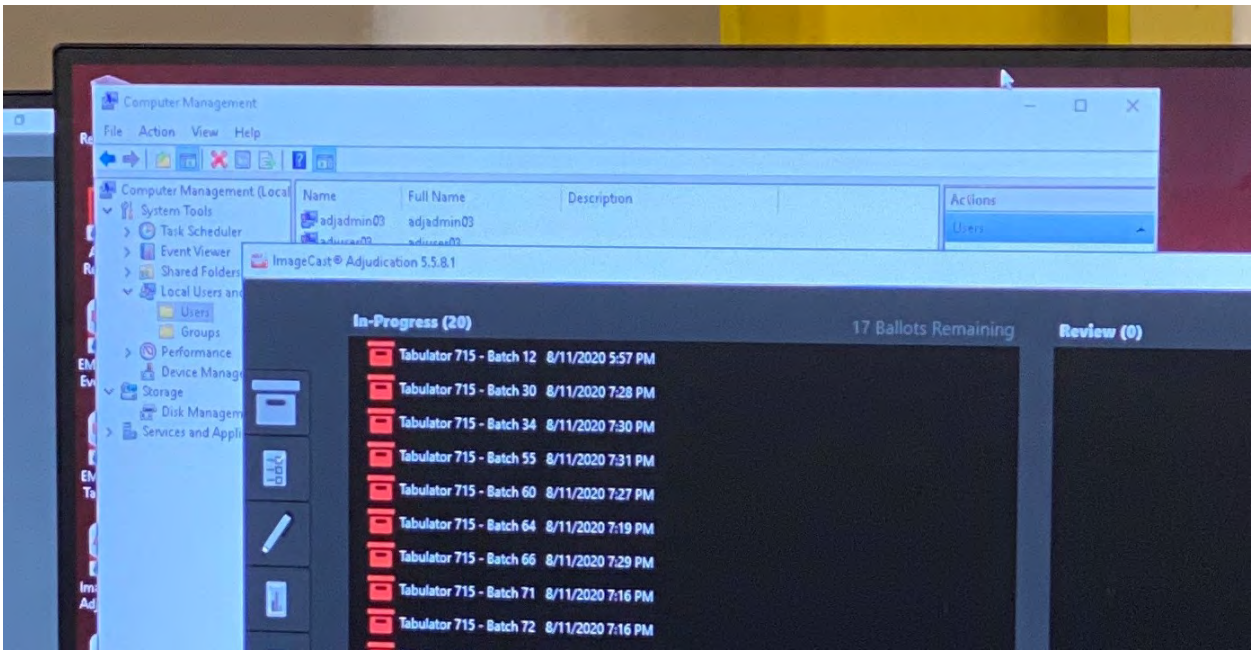

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and
Users
Groups
Performance
Device Manage
Storage
Disk Managem
Services and Appli
Name
Full Name
Description
adjadmin03
adjadmin03
Actions
Users
ImageCast® Adjudication 5.5.8.1
In-Progress (20)
17 Ballots Remaining
Review (0)
Tabulator 715 - Batch 12 8/11/2020 5:57 PM
Tabulator 715 - Batch 30 8/11/2020 7:28 PM
Tabulator 715 - Batch 34 8/11/2020 7:30 PM
Tabulator 715 - Batch 55 8/11/2020 7:31 PM
Tabulator 715 - Batch 60 8/11/2020 7:27 PM
Tabulator 715 - Batch 64 8/11/2020 7:19 PM
Tabulator 715 - Batch 66 8/11/2020 7:29 PM
Tabulator 715 - Batch 71 8/11/2020 7:16 PM
Tabulator 715 - Batch 72 8/11/2020 7:16 PM

EXHIBIT E:

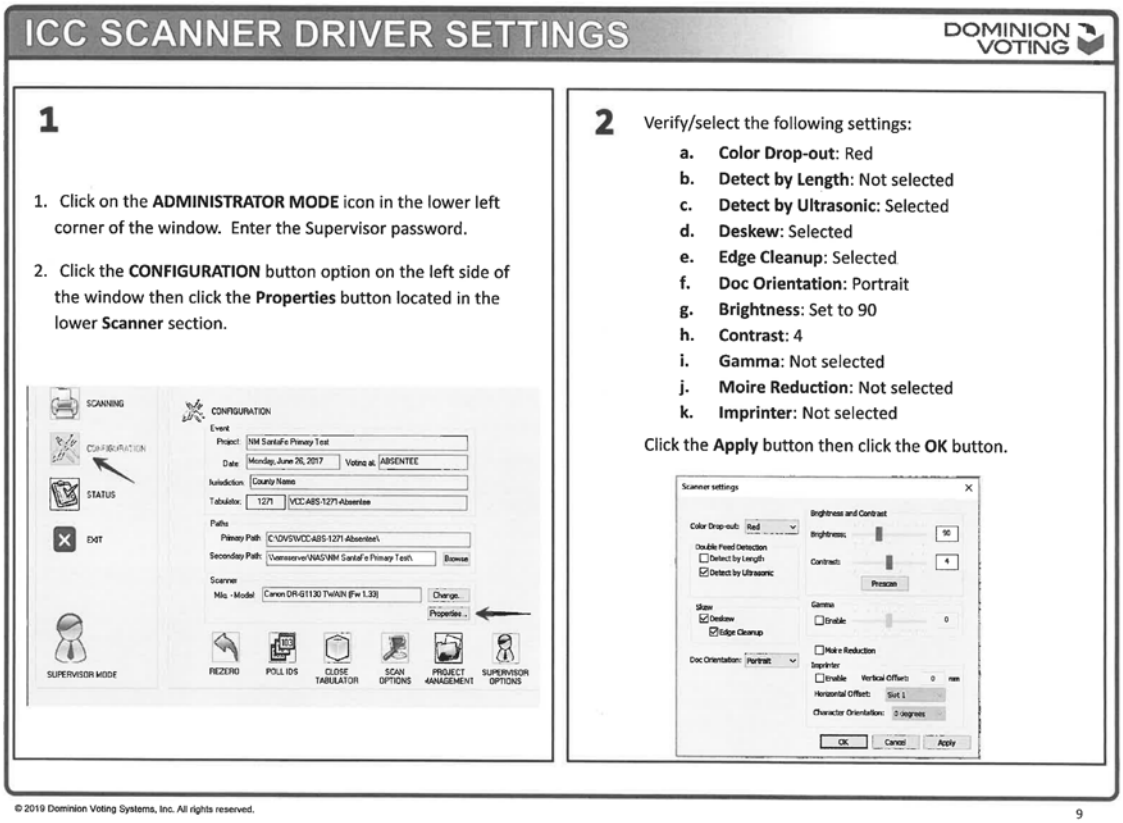

ICC SCANNER DRIVER SETTINGS
DOMINION VOTING
1
1. Click on the ADMINISTRATOR MODE icon in the lower left corner of the window. Enter the Supervisor password.
2. Click the CONFIGURATION button option on the left side of the window then click the Properties button located in the lower Scanner section.
SCANNING
CONFIGURATION
STATUS
EXIT
SUPERVISOR MODE
2
Verify/select the following settings:
a. Color Drop-out: Red
b. Detect by Length: Not selected
c. Detect by Ultrasonic: Selected
d. Deskew: Selected
e. Edge Cleanup: Selected
f. Doc Orientation: Portrait
g. Brightness: Set to 90
h. Contrast: 4
i. Gamma: Not selected
j. Moire Reduction: Not selected
k. Imprinter: Not selected
Click the Apply button then click the OK button.
© 2019 Dominion Voting Systems, Inc. All rights reserved.
9

EXHIBIT F:

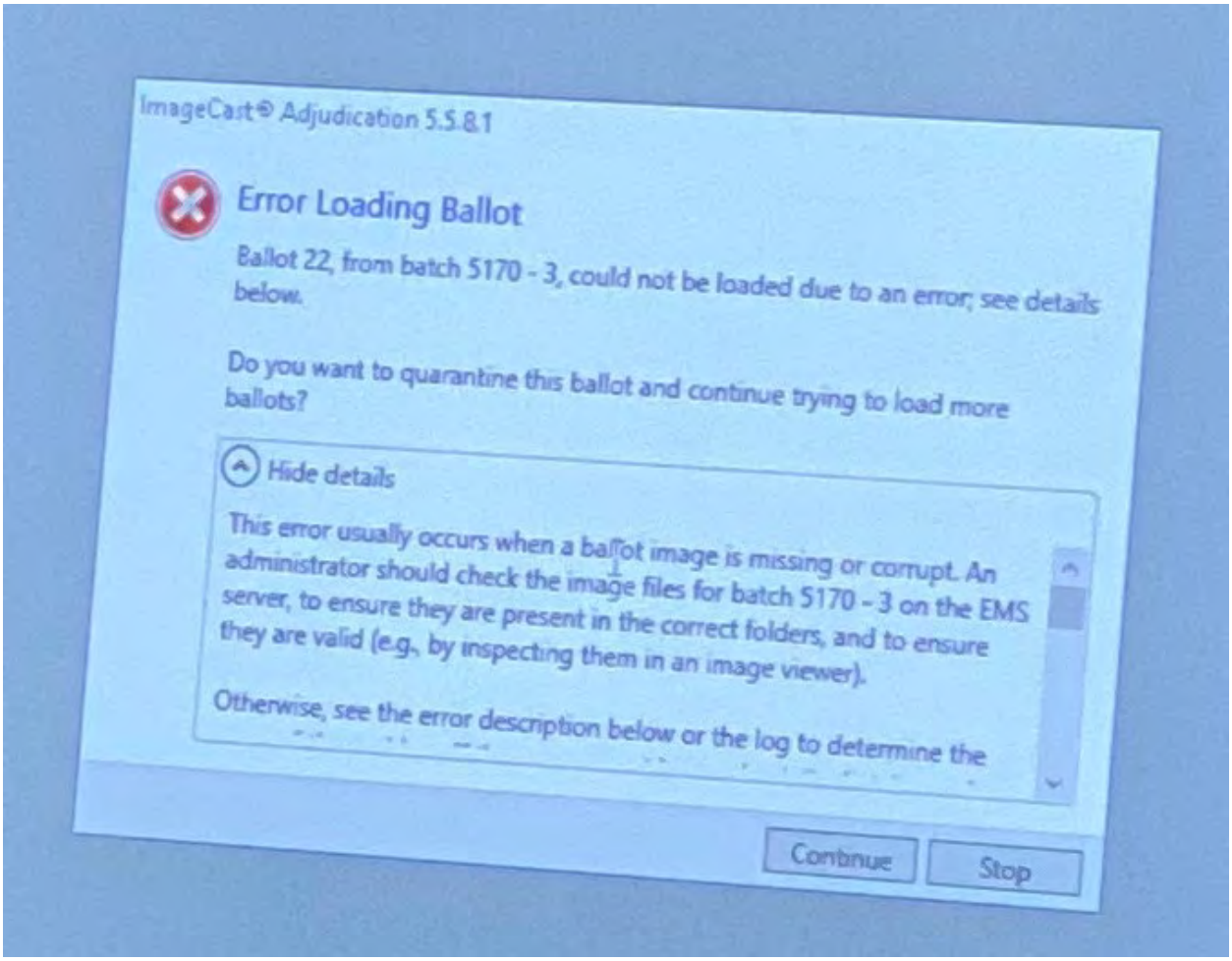

ImageCast® Adjudication 5.5.8.1
Error Loading Ballot
Ballot 22, from batch 5170 - 3, could not be loaded due to an error; see details below.
Do you want to quarantine this ballot and continue trying to load more ballots?
Hide details
This error usually occurs when a ballot image is missing or corrupt. An administrator should check the image files for batch 5170 - 3 on the EMS server, to ensure they are present in the correct folders, and to ensure they are valid (e.g., by inspecting them in an image viewer).
Otherwise, see the error description below or the log to determine the
Continue
Stop

EXHIBIT G:

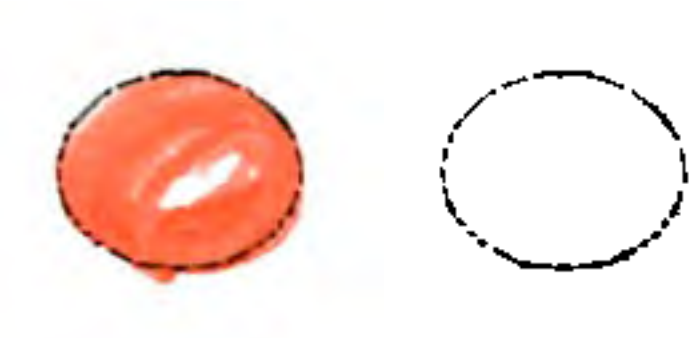
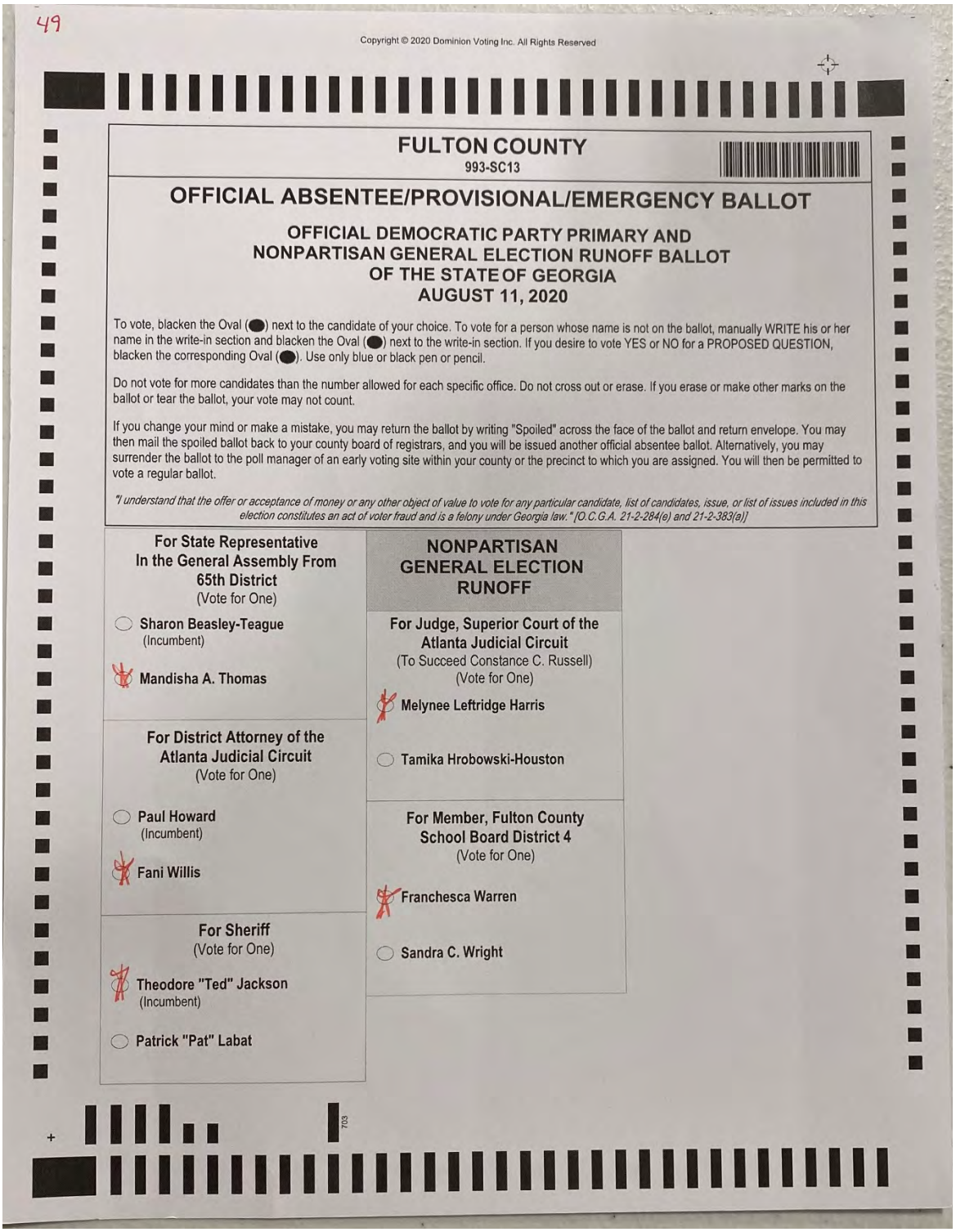


EXHIBIT H:

EXHIBIT I:



49

FULTON COUNTY
993-SC13

OFFICIAL ABSENTEE/PROVISIONAL/EMERGENCY BALLOT

OFFICIAL DEMOCRATIC PARTY PRIMARY AND
NONPARTISAN GENERAL ELECTION RUNOFF BALLOT
OF THE STATE OF GEORGIA
AUGUST 11, 2020

To vote, blacken the Oval (●) next to the candidate of your choice. To vote for a person whose name is not on the ballot, manually WRITE his or her name in the write-in section and blacken the Oval (●) next to the write-in section. If you desire to vote YES or NO for a PROPOSED QUESTION, blacken the corresponding Oval (●). Use only blue or black pen or pencil.

Do not vote for more candidates than the number allowed for each specific office. Do not cross out or erase. If you erase or make other marks on the ballot or tear the ballot, your vote may not count.

If you change your mind or make a mistake, you may return the ballot by writing "Spoiled" across the face of the ballot and return envelope. You may then mail the spoiled ballot back to your county board of registrars, and you will be issued another official absentee ballot. Alternatively, you may surrender the ballot to the poll manager of an early voting site within your county or the precinct to which you are assigned. You will then be permitted to vote a regular ballot.

"I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law." [O.C.G.A. 21-2-284(e) and 21-2-383(e)]

For State Representative In the General Assembly From 65th District
(Vote for One)

- ◯ Sharon Beasley-Teague (Incumbent)
- ✗ Mandisha A. Thomas

For District Attorney of the Atlanta Judicial Circuit
(Vote for One)

- ◯ Paul Howard (Incumbent)
- ✗ Fani Willis

For Sheriff
(Vote for One)

- ✗ Theodore "Ted" Jackson (Incumbent)
- ◯ Patrick "Pat" Labat

NONPARTISAN GENERAL ELECTION RUNOFF

For Judge, Superior Court of the Atlanta Judicial Circuit
(To Succeed Constance C. Russell)
(Vote for One)

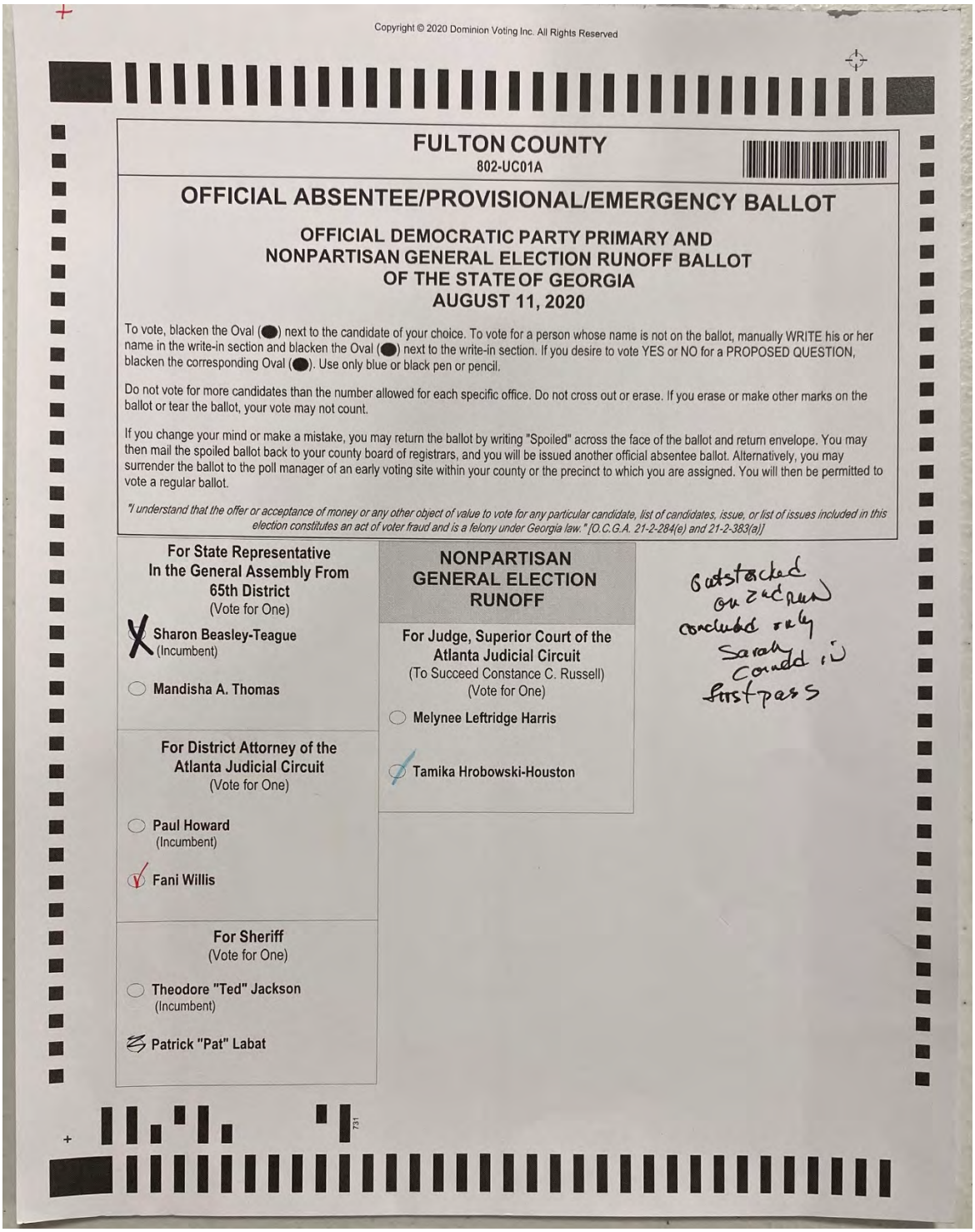
- ✗ Melynee Leftridge Harris
- ◯ Tamika Hrobowski-Houston

For Member, Fulton County School Board District 4
(Vote for One)

- ✗ Franchesca Warren
- ◯ Sandra C. Wright

703

EXHIBIT J:



FULTON COUNTY
802-UC01A

OFFICIAL ABSENTEE/PROVISIONAL/EMERGENCY BALLOT

OFFICIAL DEMOCRATIC PARTY PRIMARY AND
NONPARTISAN GENERAL ELECTION RUNOFF BALLOT
OF THE STATE OF GEORGIA
AUGUST 11, 2020

To vote, blacken the Oval (●) next to the candidate of your choice. To vote for a person whose name is not on the ballot, manually WRITE his or her name in the write-in section and blacken the Oval (●) next to the write-in section. If you desire to vote YES or NO for a PROPOSED QUESTION, blacken the corresponding Oval (●). Use only blue or black pen or pencil.

Do not vote for more candidates than the number allowed for each specific office. Do not cross out or erase. If you erase or make other marks on the ballot or tear the ballot, your vote may not count.

If you change your mind or make a mistake, you may return the ballot by writing "Spoiled" across the face of the ballot and return envelope. You may then mail the spoiled ballot back to your county board of registrars, and you will be issued another official absentee ballot. Alternatively, you may surrender the ballot to the poll manager of an early voting site within your county or the precinct to which you are assigned. You will then be permitted to vote a regular ballot.

"I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law." [O.C.G.A. 21-2-284(e) and 21-2-383(a)]

For State Representative In the General Assembly From 65th District
(Vote for One)

- [X] Sharon Beasley-Teague (Incumbent)
- [ ] Mandisha A. Thomas

For District Attorney of the Atlanta Judicial Circuit
(Vote for One)

- [ ] Paul Howard (Incumbent)
- [✓] Fani Willis

For Sheriff
(Vote for One)

- [ ] Theodore "Ted" Jackson (Incumbent)
- [S] Patrick "Pat" Labat

NONPARTISAN GENERAL ELECTION RUNOFF

For Judge, Superior Court of the Atlanta Judicial Circuit
(To Succeed Constance C. Russell)
(Vote for One)

- [ ] Melynee Leftridge Harris
- [✓] Tamika Hrobowski-Houston

Botstacked on 2nd pass concluded only Sarah counted in first pass

731

EXHIBIT K:

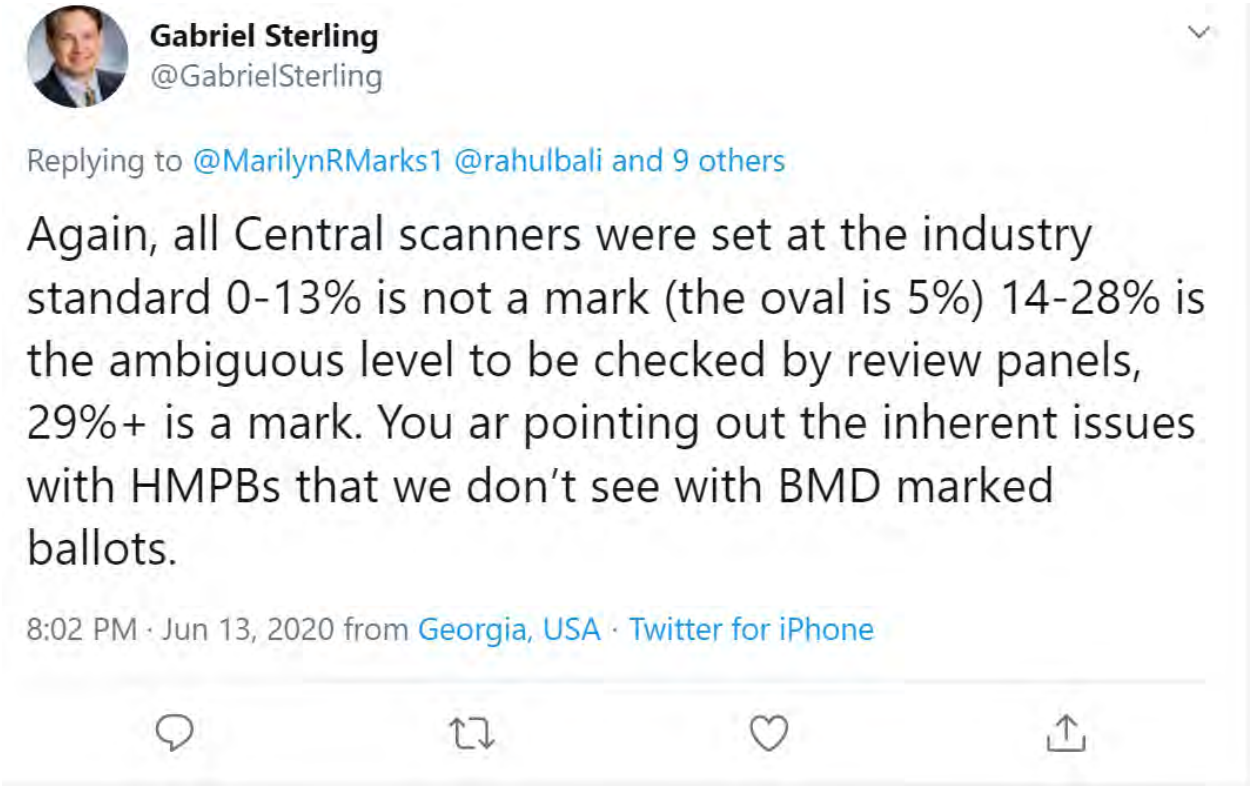

Gabriel Sterling
@GabrielSterling
Replying to @MarilynRMarks1 @rahulbali and 9 others
Again, all Central scanners were set at the industry standard 0-13% is not a mark (the oval is 5%) 14-28% is the ambiguous level to be checked by review panels, 29%+ is a mark. You ar pointing out the inherent issues with HMPBs that we don't see with BMD marked ballots.
8:02 PM · Jun 13, 2020 from Georgia, USA · Twitter for iPhone

EXHIBIT L:

- Create a voter card from Poll Pad for each unique ballot style within the designated Polling Location
  - Recommend labels be placed on card identifying what ballot style will be displayed by BMD once card is inserted
  - BMD removes the activation code from the Voter Card once used, therefore create the card again from Poll Pad after each use by a BMD

D. Testing the BMD and Printer

Use a combination of Poll Worker Card with Ballot Activation Codes for the polling location, and Voter Cards created from a Poll Pad loaded with the LA/Advance Voting dataset to bring up ballots on the BMD

- Produce at least one printed ballot from each BMD assigned to the polling location
- Produce a test deck from the BMDs assigned to the polling location for each unique ballot style within the polling location. The test deck must contain at least one vote for each candidate listed in each race within the unique ballot style
  - **Example**: Ballot from BMD 1 contains a vote for only the first candidate in each race listed on Ballot Style 1, Ballot from BMD 2 contains a vote only for the second candidate in each race on Ballot Style 1, and continue through the line of devices until all candidates in all races within the unique ballot style have received a single vote
  - **If Number of BMDs outnumber the number of vote positions on the unique ballot style**, start the vote pattern over until all BMDs have produced one printed ballot
  - **If Number of unique ballot styles in the polling place is greater than 1,** once the vote pattern is complete for a unique ballot style, proceed to the next BMD in line to start the review of the next unique Ballot Style
  - **All unique ballot styles do not have to be tested on each BMD**
- Review BMD-generated Test Deck and confirm the vote content before placing in the designated Polling Place Scanner

E. Testing the Polling Place Scanner

- Scan the BMD-generated Test Deck into the Polling Place Scanner
- Scan one blank optical scan ballot style(s) associated to the Polling Place to verify the Polling Place Scanner will recognize the ballot style in case of emergency
- Verify Scanner(s) shows a number of Ballot Cast equal to the number of ballots in the BMD-generated test deck plus the scanned blank Optical Scan ballot styles
- Firmly place the Security Key Tab in the Security Key Slot
- Touch Close Polls
- Enter the passcode
- Touch Enter
- Touch Yes
- Touch No for additional tapes (Scanner will automatically produce 3 copies of the closing tape)

EXHIBIT M:

THE DOMINION DIFFERENCE

DUAL THRESHOLD TECHNOLOGY (MARGINAL MARKS)

From its early beginnings, Dominion Voting has emphasized the use of digital scanning, and continues to set the standard in digital image acquisition and analysis in the tabulation of digitally scanned ballots. When a ballot is fed into an ImageCast® tabulator – at the precinct level or centrally - a complete duplex image is created and then analyzed for tabulation by evaluating the pixel count of a voter mark. The pixel count of each mark is compared with two thresholds (which can be defined through the Election Management System) to determine what constitutes a vote. If a mark falls above the upper threshold, it's a valid vote. If a mark falls below the lower threshold, it will not be counted as a vote.

However, if a mark falls between the two thresholds (known as the "ambiguous zone"), it will be deemed as a marginal mark and the ballot will be returned to the voter for corrective action (please see diagram below). With this feature, the voter is given the ability to determine his or her intent, not an inspection or recount board after the fact, when it is too late. The chart below illustrates the Marginal Mark threshold interpretation.

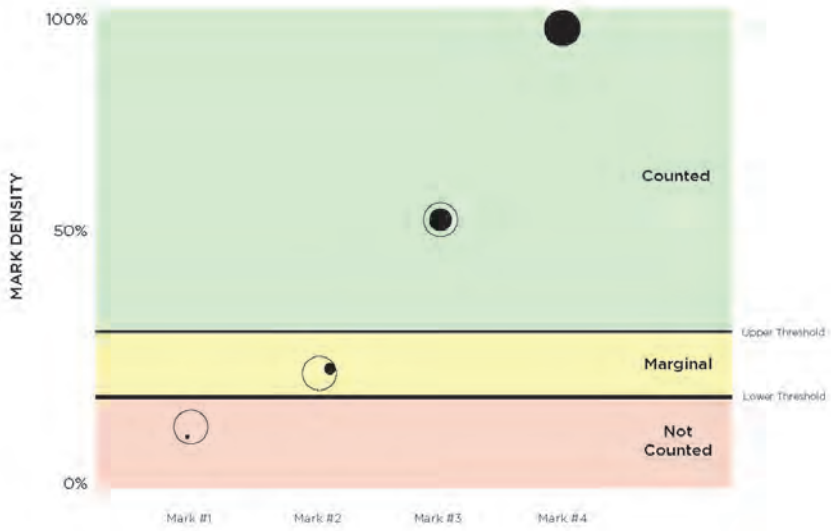


EXHIBIT 2

DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. My background and qualifications in voting system cybersecurity are set forth in my prior declaration, at Document 480-1, pages 37 *et seq.*

3. Logic and Accuracy ("L&A") Testing is a collection of pre-election procedures conducted at the county level to ensure that the voting software has been properly set up and ballots to be used in an upcoming election are properly configured. The L&A is primarily ballot specific attribute testing and is not intended to address sophisticated security, trustworthiness and other software properties' aspects of the voting system.

4. The settings instruct the software to properly display the ballot, voter instructions, collect votes, and tabulate results accurately. Therefore, the purpose of L&A testing is to test the election configuration, ballot style and other election specific settings. It is not designed or nearly robust enough for testing the software functionality, security and error free performance.

5. The software testing should be part of the election system certification testing at the federal and state level. The fact that Georgia's Dominion software (5.5-A(GA)) programming error was discovered in L&A testing undercuts the credibility of the sufficiency of certification testing that was undertaken to ensure that software will work in accordance with the specifications. Dominion Democracy Suite certification documents clearly state that the system can handle contests with over 20 candidates.

6. Based on the description given by witnesses for the State in the conference held today, the proposed process to address the software flaw discovered is not to implement the small safer modification by a patching process. Instead the proposed process seems to be replacement of the software in its entirety by overwriting the existing programming with new programming. This approach introduces highly elevated security and operational risks.

7. It has been previously described that software verification has been done in Georgia's process by reviewing self-calculated hash values on the BMDs As no additional measures were described today, I will restate that self-calculated hash values can never be used to determine and verify software integrity against malicious activity. The method can only be trusted to reveal changes and data corruption caused by non-malicious actions. It is uncontested fact that malicious software and malicious modification can cover up its presence by dishonestly

presenting expected hash value to provide false evidence that the software is genuine.

8. After new software installation, but before L&A testing, thorough functional testing should be conducted on each BMD unit to verify that the new software installation was successful and working as expected. According to State witnesses, no such testing is planned for this newly written software change. Such a minimum testing process before L&A is not an instant process and requires time to complete.

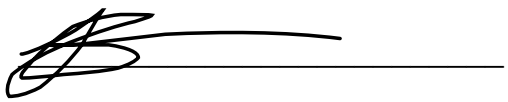
9. Software changes must always be tested both for functionality and security. From the security point of view, de minimis changes do not exist. Some of the most devasting software vulnerabilities have been matter of a single character being wrong or missing. The history of software security has countless examples of unintended consequences resulted from small changes hastily deployed without proper testing and analysis.

Conclusions

10. In my opinion the State's plan for addressing the software flaw is extraordinarily risk laden, particularly given that the new software has not even had EAC review, which is itself a low bar, but a necessary first threshold. The risk of a failed election escalates when such last minute software changes are made to an already high-risk unauditable system such as a BMD system.

11. The only reliable method of safeguarding the election from the high risk of failure is to issue hand marked paper ballots which provide the only truly resilient voting system with the ability to create a defensible election.

Executed this 28 day of September 2020.



Harri Hursti

DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, HARRI HURSTI declares under penalty of perjury that the following is true and correct:

1. This declaration supplements my prior declarations (Docs. 680-1, 800-2, 809-3, 860-1, 877, and 923-2) a nd I stand by the statements in those declarations.

2. I arrived at the Fulton County Election Preparation Center ("EPC") on October 1, 2020 around 3:45pm. I was there in my capacity as an expert engaged by the Coalition Plaintiffs to conduct a Rule 34 inspection. (Exhibit 1) . I was accompanied during part of my visit by Marilyn Marks of Coalition for Good Governance.

3. My goal for this observation and inspection was to review the ongoing updating of the Dominion software for Fulton County ballot marking device ("BMD") touchscreen units to ICX software version 5.5.10.32. It is my understanding that Fulton has an inventory of over 3,300 BMD touchscreens, all of which are to be updated with this software. A number of the machines were in the EPC warehouse and were staged to be updated or marked after the update had been completed.

4. Upon our arrival, Ms. Marks and I were informed by Derrick Gilstrap, the manager of EPC, that all of the people working to upgrade the devices were

Dominion technicians. Mr. Gilstrap stated that he did not feel comfortable installing a last-minute software change, and did not want Fulton County staff to be responsible for installing it. He told us that he told Dominion to conduct this operation, prior to having his staff install the November 2020 election programming and Logic and Accuracy testing ("LAT").

5. Mr. Gilstrap told us that after the software update step that LAT would immediately begin, and made no mention of Acceptance Testing that should occur prior to LAT.

6. Acceptance Testing is an almost universally mandated basic test of the hardware and software when a change or repair to either has been made before counties are permitted to install election programming and deploy voting system components. Acceptance testing must be performed on each unit, and cannot be performed on a sample basis. Fulton's failure to conduct such testing should be a serious warning sign of further recklessness in the installation of inadequately tested software.

7. Mr. Gilstrap stated that Dominion had started the software update project with four workers, but soon realized that the task would take extended periods of time. Mr. Gilstrap stated that Dominion had accordingly increased the workforce to 14 and expected the installation work to be completed on Monday, October 5.

8. The new software was contained on USB sticks. However, there was no inventory management present for the USB sticks. There also was no inventory control for the technician authorization smartcards, which provide access to the controls of the touchscreen. Workers did not sign or otherwise document when they took possession or returned the technician cards and software upgrade USB sticks. Those items were in an open plastic bag which was sometimes placed on table, and sometimes carried around the working area by the manager. Anyone was able to pick up a USB stick or drop them there freely, permitting the easy substitution of USB sticks containing malware or to leave the premises with copies of the software update.

9. Some workers worked one BMD touchscreen machine at the time, while others simultaneously worked on 2 or 3 machines. There was no accountability for how many sticks and technician smart-cards each worker had in their possession. Clearly, the USB sticks were not considered to be security sensitive items at all.

10. Some of the workers had instructions for software update visible in their pockets, while others did not seem to have the instructions readily available. One worker showed me the instructions, but it was different from the instructions I had seen that were sent to the counties. None of the technicians that I observed were following the instructions as they installed the new software.

11. Technicians were not following a common process, and they all made their own variations on the workflow. In my experience, this can negatively affect the quality and reliability of the software installation. Many workers were texting and making phone calls while working and not focusing on their work. As a result, I observed repeated human errors such as skipping steps of the process.

12. Some workers consistently took an extra step to destroy previous application data before uninstalling the old version of the software. Uninstalling software packages results in destroying application data, but that is known to be unreliable in old versions of Android. The step they took is ensuring, among other things, destruction of forensic evidence of Fulton's use of the equipment in prior elections.

13. To avoid destruction of all forensic evidence from the BMDs, a number of images of the electronic data contained on the BMDs should be taken from a sample of them before installation of the new software.

14. As part of the updating process, the workers are directed to enable the "Install from Unknown Sources" setting. This is an insecure mode because it turns off the operating system verification of trusted sources and therefore allows software from any source to be installed. During the 45 minutes of my observation, I observed that many units had been left in insecure mode. I estimate 15% of the units were already in the insecure mode when the work began on them, having

been left that way during the last software installations, or because of interim tampering.

15. As described before, most workers I observed were not focusing on the work they were tasked to do, and as result, they were accidentally skipping steps. I observed that, as result of these human errors, the units were erroneously left in the insecure mode either by the workers skipping the step to place the machine into the secure mode after upgrade, or doing the step at such a fast pace that the system did not register the touch to toggle the switch and the worker did not stop to verify the action.

16. The State Defendants and Dominion have repeatedly overstated the value of their hash test, but my observation showed that they themselves are not relying on such test as a control measure. Dominion workers are not even checking the hash value. I deliberately followed many workers when they processed the units. During over 45 minutes of observation, none of the workers took the step of verifying the hash value. Some workers did not realize that the upgrade had failed and the mistake was only caught by persons who were closing the cabinets when and if they looked at the software version numbers before closing the doors.

17. I also observed random errors that were not caused by humans. For example, software sometimes refused to uninstall because the uninstall button was

disabled, or the installation silently failed. The technicians treated devices with issues by simply rebooting them. Technicians made no effort to diagnose or document the cause of the issues. The casual nature of dealing with the irregularities caused me to conclude that these abnormal incidents are commonplace.

18. Based on my observations of the software update, I would anticipate that these machines are likely to behave inconsistently in the polling place, depending on a number of factors including the care taken in the software installation process.

19. The current abbreviated LAT protocol adopted by Fulton County and the State cannot be relied on to identify problems created by the new software or its installation (or other problems with programming and configuration unrelated to the new software). Even if counties were conducting the full LAT required, it is but one step that is needed, and is quite insufficient for ensuring the reliability of the BMD touchscreens—which at the end of the day, simply cannot be done.

20. In my professional opinion, the methods and processes of adopting and installing this software change is completely unacceptable. The methods and processes adopted by Dominion and Fulton County do not meet national standards for managing voting system technical problems and remedies, and should not be accepted for use in a public election under any circumstances.

21. It is important that full details of the software change made be available for analysis and testing to determine the potential impact of the changes. I concur with Dr. Halderman's opinion in Paragraph 8 of his September 28, 2020 declaration (Doc. 923-1), in which he states that if the problem is as limited as described by Dominion, it could have been addressed with far less risk by the State without making an uncertified, untested software change.

22. In my opinion, the installation of the last-minute software change adds intolerable risk to the upcoming election, and the simple solution of removing the BMD units from the process and adopting hand marked paper ballots is imperative.

23. I note that I wanted to document the upgrading process, but Mr. Gilstrap told me that I was prohibited from taking photographs or video. I showed him the Rule 34 inspection document and pointed out the paragraph permitting photographing. He read that carefully but told me that he needed to clear that with his superiors before I could start taking pictures. He never cleared this with his superiors while we were there.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 4th day of October, 2020 in Atlanta, Georgia.

Harri Hursti

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct:

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. This declaration supplements my prior declarations (Docs. 680-1, 800-2, 809-3, 860-1, 877, 923-2, and 942 at 7) and I stand by the statements in those declarations.

3. This declaration is written to explain and support the Coalition Plaintiffs' request for relief to address uncounted valid hand marked votes and the Court's Order to provide specific recommendations (Doc. 964 at 141).

4. In my opinion, it is quite feasible to make immediate changes to increase the accuracy in vote detection and tabulation of hand marked paper ballots scanned by the Dominion ICC scanner. As I had expected based upon a review of the system documentation, programming and database building are not required for the simple changes that I recommend. This has now been verified by my testing in Cherokee County.

5. My recommendation for substantial near-term improvement in vote detection and vote counting is for each county to change the Dominion ICC scanner Brightness setting to a value of 25, and maintain the Contrast setting value of 4, which appears to be the vendor default value. This change may be made by the voting system administrator in each county before scanning a batch of ballots. This recommendation assumes that counties are using the same type of ICC scanner (Canon DR-G2140) and same type of ballot paper stock provided by Cherokee County for my test.

6. The Dominion County Users Guide 5.5A distributed to the counties contains the instructions for changing these values by county administrators.

(Exhibit 1). Based on observations in Cherokee County, this action would require less than 5 minutes of staff time, including a brief test. I will explain below the basis for the recommendation.

Background Regarding My Work With Georgia's Scanner Settings

7. As stated in my Declaration of August 24, 2020 (809-3 ¶52), I initially heard about the failure of the Georgia's Dominion system to detect and count all legitimate votes in early June 2020 from Marilyn Marks and Jeanne Dufort of Coalition for Good Governance.

8. Ms. Marks also informed me of such vote counting problems she had observed in the Habersham County June 9 recount. Such problems reportedly occurred because of marginal marks not recognized as votes by the system. After these repeated reports of uncounted votes on hand marked scanned ballots in multiple counties, I began to gather information on potential sources of the scanning problem.

9. Ms. Marks arranged a video call with Richard Barron of Fulton County, Dr. Richard DeMillo, Ms. Marks and me on June 27, 2020. The purpose of the call was for Dr. DeMillo and me to offer assistance to Fulton County to analyze the cause of the uncounted votes experienced in the June 9 primary and mitigate the uncounted vote issue with more appropriate scanner settings. (Dr.

DeMillo has considerable expertise in scanning technology, particularly given his executive experience at Hewlett-Packard.) Dr. DeMillo and I suggested to Mr. Barron that we work as a team during Fulton's upcoming preparations and Logic and Accuracy Testing for the August 11 runoff to test various combinations of settings to optimize vote counting accuracy. Our offers to help were declined by Fulton.

10. On July 1, 2020 Ms. Marks forwarded a copy of Exhibit 2, which is a document describing Dominion scanner configuration produced by Henry County in response to an Open Records Act request for such documents supplied to the county by the Secretary of State. Exhibit 2 details a number of scanner setting changes that can be made by the local election official.

11. In July and August, Coalition Plaintiffs requested through a Rule 34 inspection that Fulton County permit me to conduct several hours of testing on the ICC scanners to improve the vote count accuracy. This culminated in a discovery dispute (Doc. 839) which has not been resolved. Therefore, I have been unable to conduct the full range of testing that is necessary to recommend ***optimal settings*** on all available parameters, such as thresholds, dpi, grayscale, gamma, brightness, contrast, and other technical options. Such comprehensive testing is not only for the purpose of finding the best settings for capturing votes, but to verify that the

new settings will not produce unintended adverse effects like reduced speed, false positives or decrease in ballot timing mark recognition reliability.

12. Although I have been unable to test and verify the optimal settings, the recommendations described in this declaration will measurably improve the accuracy in vote detection and tabulation of hand marked paper ballots scanned by the Dominion ICC scanner and can and should be made immediately. These recommendations are based on the testing I conducted using November 3, 2020 Cherokee County test ballots scanned in Cherokee County Election Office on September 29 and October 20 and my independent research. I will explain the details of my Cherokee County scanning testing below.

Scanner Settings Adjustment Feasibility

13. I demonstrated through the Cherokee testing the feasibility of immediate improvement in scanning and tabulation accuracy for ballots scanned by the ICC. My findings are contrary to Dr. Eric Coomer's and Defendants' testimony and declarations, which implied that any settings changes to create scanning improvements required long lead times and database programming prior to an election. In fact, I demonstrated that database or programming changes are not necessary to make near-term significant improvements.

14. Dr. Coomer stated in his testimony of September 11, 2020 that, "Whether a mark is characterized as a ballot vote, an ambiguous mark, or not a vote is wholly dependent on the threshold settings of the lower and upper threshold limits as well as the percentage fill of the target detected by the system." (Transcript p.72 lines 21-25)

15. Dr. Coomer's statement implies that improvements to vote detection and counting accuracy can only be achieved by changing the threshold settings while building the database. Instead, my testing proved that a simple change to the Brightness setting to 25 from the apparent default value of 90 recommended by Dominion will result in significantly better vote detection accuracy in Georgia. Scanner manufacturers use 100 as the factory default, with intention that all their scanners produce similar results with factory default settings. Dominion's recommended defaults differ from factory default for the Canon G-DR2140.

16. Dr. Coomer states in his declaration of August 28, 2020 (Doc 834-1) that, "Scanner threshold settings for the Dominion Democracy Suite that Georgia purchased are not set on each individual scanners. Instead, scanner threshold settings are set when the voting database is built. Users are not able to change the threshold settings without being trained to do so, and with the appropriate application access privileges." His assertion should not be read to mean that

threshold settings are the correct or only settings that can be changed to improve vote detection, or that counties have no convenient access to make setting adjustments to do so.

17. It is my understanding that, after vote counting issues related to marginal marks were exposed in the June 9 primary, the State Election Board required adjustment of the threshold settings, which was explained in the Court hearing on September 11, 2020. The new threshold settings were applied to the November 3, 2020 election configuration, including in the election project for Cherokee County. Those new threshold settings would have been utilized during my testing at Cherokee.

18. My testing demonstrated that the State's recent adjustment of threshold settings was insufficient to detect and count all reasonably detectable legitimate vote marks.

19. As I describe below, changing certain scanner settings is always available to any county voting system administrator with administrative credentials, using simple instructions in the user manual. Attached as Exhibit 1 is a copy of two pages of instructions from the Georgia County Users Guide 5.5A which I photographed in Cherokee County on October 20, 2020. The software providing the ability to change the scanner settings on Exhibit 1 page 2 is not

software used in defining the database. The readily adjustable settings listed on the display screen that can have an impact upon image quality include brightness, contrast, gamma, moire reduction, deskew, and color dropout among others. Canon scanner manuals reveal a wide range of additional settings, which are not displayed for user changes in the Dominion interface to Canon scanner. The default values and their effect on ballot scanning are not disclosed in the Dominion reference material I have reviewed. These currently hidden settings affect the scanner operations.

20. Inspecting the configuration and conducting testing in Cherokee reinforced my previous belief, after a review of publicly available materials, that such scanner setting adjustments may be made by county election staff at any point in the election. My Declaration of August 24, 2020 explains the fact that "important image processing are done in scanner software and before election software threshold values are applied to the image." (Doc. 809-3 at 25).

21. It is my understanding that there are no state rules or requirements that prohibit the counties from making changes to these settings.

22. I strongly recommend that, after the interim setting changes recommended in this declaration are implemented for near-term improvements, optimal settings should as soon as possible thereafter be determined and further

ordered to be implemented as uniform mandated settings with state permission required before any county level changes are thereafter allowed. Otherwise, counties could effectively unintentionally create differing vote detection standards, where not all voters' ballots are tabulated in the same manner, worsening the problem that now exists with different standards between manual and on screen adjudication processes by the Vote Review Panels.

23. My recommendation is subject to my understanding that Dominion is using the same certified ICC scanner model in all counties, and all counties are using the same Dominion approved paper stock for ballots scanned on the ICC scanners, and that the Cherokee testing environment was the standard operational election setup used in all counties.

Changing the Brightness Setting

24. To make the recommended change to the Brightness setting (that is, from 90 to 25), County voting system administrators can reference pages 125-126 of their Dominion Georgia County Users Guide 5.5A Section 4.4.7. These pages include diagrams showing how to adjust the brightness setting to the recommended value of 25. (Exhibit 2). Such a setting change can be made and tested in less than 5 minutes in my opinion based on my observation of Cherokee County.

Cherokee County Scanning and Testing

25. Along with Marilyn Marks and Aileen Nakamura of Coalition for Good Governance, I made two visits to the Cherokee County elections facility for the purpose of conducting some basic scanning testing. The first visit was on September 29, 2020 and the second visit was on October 20, 2020. The second visit was permitted for two hours by Court Order (Doc.977).

26. I arrived at the Cherokee County elections facility on October 20 at 5:40pm and testing session began at approximately 5:55 pm. In attendance were also Ms. Ann Brumbaugh, attorney for Cherokee County; two members of the Cherokee County Board of Elections (whose names I failed to record); Mr. Brad Skelton of Dominion; Mr. Bryan Jacoutot, an attorney representing the Secretary of State; Ms. Kim Stancil, Cherokee County Director of Elections; Ms. Jennifer Akins, Assistant Election Director of Cherokee County. Ms. Nakamura recorded video of the session.

27. At the beginning of the session, Dominion regional manager, Brad Skelton insisted repeatedly that Brightness and Contrast settings are set "in programming" and cannot be changed at the county level. Ms. Brumbaugh and Ms. Marks questioned him repeatedly about his statement that the settings were done in programming. Ms. Marks reminded him that, to the contrary, the user's manual

information obtained from Henry County showed that counties could make such settings changes.

28. I had downloaded the Dominion ICC user manual (Democracy Suite® ImageCast® Central User Guide") from the Secretary of State of Colorado's website, which may be found at https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf. I had also reread Exhibit 2, which is the directions for preparing the scanner for an election and changing scanner settings supplied to Coalition for Good Governance by Henry County. (This document is discussed in my prior declaration, Doc. 809-3 ¶ 59). Both documents indicated that the settings can be changed at any time and are not part of the programming or the database.

29. Ms. Akins permitted us to review the Dominion Georgia County User Manual 5.5-A which was by the workstation in a binder. Within a few minutes I was able to find the correct pages from the index explaining how to make adjustments to Brightness and Contrast settings. The settings listed on page 126 of the manual (Exhibit 1 page 2) do not require an election project database change or programming change, contrary to what was indicated by Mr. Skelton and implied by Dr. Coomer. In fact, the setting may be changed any time and even every ballot

batch may be scanned with different settings by an operator. The software used to change these settings is not used to create the database.

30. In preparation for the on-site testing, I had prepared a computer simulation of 40,000 images of ballot-type mark variations to estimate what the optimal ICC settings would be. Based on the simulation I expected that the optimal setting would be approximately -89% brightness and +62% contrast.

31. I found the settings on the Cherokee Dominion ICC scanner were displayed in the dialogue box as “90” for Brightness, (providing an effect of -10% brightness), and “4” for Contrast. Those values are the same as those shown in the diagram in Exhibit 1 page 2.

32. From the ballot vote-mark detection point of view alone, -99% brightness provided the optimal reading of the vote targets, but as an unintended consequence, it enhanced printed extraneous marks on the ballots. There extraneous marks were printshop production aid landmarks and the Dominion copyright text. These markings are outside of the ballot timing marks area and when enhanced, confused the software interpretation of the timing marks on the borders of the printed ballot. (Exhibit 6) This assumption is based on the pre-scan feature of the software which offers additional information how the software is analyzing the ballot.

33. During the scanning testing, I found that numeric Brightness setting 25 providing an effect of -75% yielded most of the benefits without any discernable negative impact on reliability of ballot detection while providing improvements in vote detection. No other settings were changed from the Georgia default settings.

34. We scanned the test ballot deck generating about 400 front and back scans with this Brightness setting of 25 (without changing other settings) without a single error message.

The Test Deck

35. The test deck consisted 43 paper ballots for the November 3, 2020 election obtained from Cherokee County Elections Office. Marilyn Marks and I marked the ballots creating the test deck prior to the test session. As a testing control, we marked each ballot with a one control mark along with standard and non-standard markings. A control mark is well-marked target area using a black pen.

36. Ms. Marks and I made other marks on the test ballots to simulate marks that voters may make with many marks deliberately intended to test detection boundaries. This included markings with approximately 20 different kinds of writing instruments--different ink colors, types of pen and different widths

of the tip. We made "X marks," "check marks," slashes, circles around the target areas, highlighted the candidate name, and other standard and non-standard markings, and used differing pressure on the paper ballot. We also made markings with different alignments in relationship to the center of the oval target area and purposefully created overvotes by making hesitation dots in some already marked contests.

37. The test deck was scanned multiple times in different orientations. "Orientation" in this case means head-first vs tail-first and front-side up and down.

38. The operator, Jennifer Akins, did not save every scanning result, because part of the intention of the test was to test reliability of the scanning operation. No images were rejected based on the content of the ballot image. It was not necessary to retain every scan iteration. The baseline images for the entire deck scanned with the default settings were preserved, as were images in the deck run with the recommended Brightness setting of 25.

39. A total of 513 ballot images, including both sides and the election software interpretation of the ballot, (with many vote markings on each page) were saved for the analysis.

Results

40. Changing the Brightness setting to 25 resulted in additional vote marks being detected and accepted as votes on 38 out of 43 test ballots. An example of detecting votes using the changed Brightness setting only is shown in Exhibit 3. Using Test Ballot #55 marked with a black pen, the recommended Brightness significantly increased vote detection from having 20 blank races on the current default settings to having only 4 blank races.

41. On 6 ballots certain vote mark anomalies, which were previously ignored, were now detected. The test deck contained possible overvotes which previously had not been detected, and improved setting allowed the election software to detect those.

42. No false positive marks were detected and counted as votes.

43. Exhibit 5-1 shows how the scanner still removes highlighter marker marks, but now the scanner image processing software makes both the vote target oval and the candidate text to appear as bold. This illustrates how the scanner is not taking pictures of the ballots but processes the images with its own hidden logic, which has not been made available to me to evaluate. Similar effects were seen also with yellow highlight, but not as prominently.

44. Even with the brightness changed to 25, some marks failed to be detected, as should be expected in an actual election. I would not expect that the

Dominion ICC scanner system could be set to accurately detect and analyze every possible mark as long as the images are reduced to have bi-level data only (i.e., black and white). Even with color or gray-scale scanning, some human review of marginally marked ballots will always be necessary. I recommend that in recounts or very close races, that ballots be manually examined prior scanning, in order to inspect for such marginal marks in specific races. It is my understanding that Georgia does not require this safety measure.

45. But after such a quality improvement, review can be done more reliably from the images without need to observe the physical paper ballot in most cases, if results are not close. Auditing election results, including Risk-Limiting Audits will always require visual inspection of the physical ballots.

Findings Causing Concern

46. On multiple test ballots, the scanning captured markings outside of the oval, but markings inside of the oval disappeared, and no vote was recorded. The root cause for why software appeared to be erasing markings from inside of the oval should be investigated. This phenomena is not limited to red color markings, while it exhibits itself more prominently with red markings. (Exhibit 4)

47. My testing revealed similar integrity and accuracy issues with unmodified settings as was discovered with the ICP (precinct scanner). At times,

ballots scanned and rescanned in different orientations produce different results. Changing the brightness setting improved reliability but did not eliminate the issue of different orientation generating different results. For example, in Exhibit 3, the test ballot #55 was falsely producing from 18 to 20 blank races (no vote detection) with the vendor settings and with improved settings 4 to 9 blank races when the same ballot was rescanned in different orientations. But with both settings, the ballot was interpreted inconsistently on each scan. Given that all markings on this sample ballot were done with black or blue pens, the brightness change demonstrates the benefits even when recommended pens are being used. Exhibit 3. However, the root cause of this effect should be investigated and addressed by Dominion.

48. Dr. Coomer testified that an increase in the target oval's line width would cause the oval vote target to register as a vote (Transcript Sept. 11 p 125-126) TranHowever, my testing demonstrates that it is not the case. Ovals with significant increase of widths, and therefore black marking, still did not register as votes. Exhibit 5-1

49. As I expected, the enhanced Brightness settings are still failing to detect some non-standard but legitimate votes, despite the significant improvement the change created.

Other Impacts of Setting Changes

50. I anticipate that increasing the vote detection through the Brightness setting will significantly reduce the workload of the Vote Review Panels because the number of ballot marks required to be adjudicated should be reduced. This work reduction will be true for both counties adjudicating by manually reviewing the original ballots and those using the on-screen adjudication of ballot images.

51. Another benefit of the increased vote detection through the recommended scanner setting changes will be that the results of vote counting processes in counties that use manual adjudication will be more consistent with the less accurate method of vote counting by counties using on-screen adjudication. The manual method should be more accurate in that if any marginal marks are detected by the scanner, the entire ballot is duplicated manually with all marks inspected and duplicated by the panel. Panels using only on-screen adjudication from low quality images can easily miss marks that are not flagged for review or those that are not detected by the scanner.

Conclusions

52. The state's narrowing of the dual threshold values did not adequately address the problem of the system's failure to count certain legitimate vote marks.

53. Setting the brightness to 25 significantly increases non-standard mark recognition without negative impact on reliability or speed of the scanning.

54. The scanner setting can be changed at the county level in less than 5 minutes.

55. I recommend that counties be instructed to immediately begin scanning hand marked ballots using a Brightness level of 25 and Contrast level of 4 on the ICC scanner, and that the other default ICC settings be maintained at present.

56. If there are concerns that some ballots already scanned may have a less accurate vote detection process, and if for some reason these ballots cannot simply be rescanned using the updated settings, then I recommend that races with results within 1% be rescanned on the improved setting prior to certification.

57. Alternatively, in the event that county officials cannot undertake this brightness scanning adjustment in time for the November election, I recommend that uncounted votes in close races be mitigated using the following option. For any race within a 1% difference of the hand marked ballot count between the two top candidates, the ballots should be rescanned using the new settings for those

specific races with undervote detection turned on to detect potential uncounted votes in very close races.

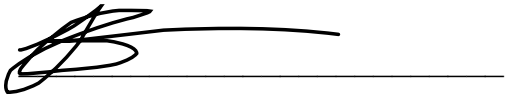
58. Future study to find optimal values using the total combination of available local settings of brightness contrast and gamma should be conducted and settings tested for future elections before databases are built. Other settings for grayscale, threshold, and dpi should be tested and optimized simultaneously. All settings are subject to the exact type of scanner being used and the type of paper used as ballot paper.

59. Testing should be conducted to determine if extraneous markings on the ballot (such as the trademark) can be removed in the scanning process to use more effective settings to further increase the vote recognition without negative impact on reliability. (Exhibit 6)

60. Although these scanner settings (such as Brightness and Contrast) are easy to change, they are not easy to monitor by election officials or authorized tabulation observers. I therefore further recommend that the settings be prominently displayed as a matter of election integrity and security, because they are so easily changed and can have a major impact on tabulation accuracy. An unnecessary risk to election integrity and security is present when election staff

operating the scanner is unable to easily to verify the settings during the scanning process.

Executed this 26th day of October, 2020



Harri Hursti

EXHIBIT C

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

DONNA CURLING, an individual, et al. Plaintiffs, v. BRIAN P. KEMP, in his individual capacity and his official capacity as Secretary of State of Georgia and Chair of the STATE ELECTION BOARD, et al., Defendants.	)	CIVIL ACTION FILE NO.:

AFFIDAVIT OF LOGAN LAMB

County of Fulton)
) ss.
State of Georgia)

LOGAN LAMB ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am a cybersecurity researcher based in Atlanta. I have a BS and MS in computer engineering from University of Tennessee, Knoxville. I have worked professionally in cybersecurity since 2010. I started at Oak Ridge National Lab in the Cyber and Information Security Research group. At CISR I specialized in static and symbolic analysis of binaries. I also worked with embedded systems security and conducting security assessments for the federal government. I left ORNL in 2014 and joined Bastille Networks, a local startup where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

2. On August 23, 2016 I went to 130 Peachtree Street in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conducting a wireless security

assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment is managed by the Center for Election Systems at KSU.

3. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the Center for Election Systems public website to see if there were any public documents that could give me background on CES and Merle King. I used the search "site:elections.kennesaw.edu inurl:pdf" at www.google.com and discovered what appeared to be files relating to voter registration cached by google.

4. After this discovery, I wrote a quick script to download what public files were available here: https://elections.kennesaw.edu/sites/ , at the time a publicly accessible site. After running the script to completion I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:

- voter registration databases filled with personally identifiable information of voters (filename *PollData.db3*)
- Election Management System GEMs databases (.gbf and .mdb extensions)
- PDFs of election day supervisor passwords, for example:
    - *July 2016 Primary and NP Election Runoff Password Memo.pdf*
- Windows executables and DLLs, for example:
    - *System.Data.SQLite.DLL*
    - *ExpDbCreate.exe*
    - *ExpReport.exe*

5. Besides leaking information, the server at elections.kennesaw.edu was running a version of Drupal vulnerable to an exploit called drupageddon. Using drupageddon, an attacker can fully compromise a vulnerable server with ease. A

public advisory for drupageddon was release in 2014, alerting users that attackers would be able to execute, create, modify, and delete anything on the server.

On August 28, 2016 I sent an email to Merle King notifying him of the vulnerabilities I found.

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: https://www.bastille.net/. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"
I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install. Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"
The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
https://www.drupal.org/project/drupalgeddon
https://www.drupal.org/SA-CORE-2014-005

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

6. After having a brief conversation with Mr. King on August 29, 2016 and being assured that the issues would be remediated, I dropped the issue.

7. In late February, 2017 I told my colleague Chris Grayson about what transpired in August. He quickly confirmed the leaking of information had not been appropriately remediated. I tweaked my script and checked to see if it worked as it had in August.

8. The script was able to download the publicly available information. The data downloaded included the same data from the previous collection and new information relating to recent elections including:
   - More recent GEMs database files
   - Files relating to the presidential election, e.g.
     - *November 2016 General Election Day Password Memo.pdf*
     - *November 2016 General Voter Lookup Password Memo.pdf*
   - Very recent files, e.g. *064 (1-10-2017).pdf*

9. Given the severity and ease with which an attacker can use drupageddon, an attacker would have easily been able to gain full control of the server at elections.kennesaw.edu had they so wanted.

10. Having gained control of the server, an attacker could modify files that are downloaded by the end users of the website, potentially spreading malware to everyone who downloaded files from the website.

11. In addition to the previously mentioned files on the server, there were multiple training videos. One of these training videos instructed users to first download files from the elections.kennesaw.edu website, put those files on a memory card, and insert that card into their local county voting systems.

12. Further Affiant sayeth not.

Logan Lamb

Sworn before me this 30 day of June, 2017, in June.

NOTARY PUBLIC

EDWARD TINSLEY NOTARY PUBLIC EXPIRES GEORGIA July 23, 2019 FULTON COUNTY

DECLARATION OF LOGAN LAMB

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF LOGAN LAMB

LOGAN LAMB hereby declares as follows:

1. I am a cybersecurity researcher based in Atlanta, Georgia.

2. I have a Bachelor of Science degree and a Master of Science in computer engineering from University of Tennessee, Knoxville.

3. I have worked professionally in cybersecurity since 2010 where I started at Oak Ridge National Lab in the Cyber and Information Security Research group. In that position, I specialized in static and symbolic analysis of binaries, red-teaming prototype critical infrastructure, and de-identifying geospatial data.

4. I left that operation in 2014 and joined Bastille Networks, a local cyber-security startup business where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

DREs are not and will never be secure

5. A DRE (direct-recording electronic) is a voting machine which records votes electronically. DREs do not have a voter-verified paper audit trail, meaning there

is no way of auditing the results of an election. A voter-verified paper audit trail allows voters to independently verify that their vote is being recorded as intended, which is impossible with DREs since the sole record is an electronic copy, and the voter cannot determine how his vote was recorded. Since the only copy of the electronic vote is stored on the machine, there is no way to independently verify the votes cast by voters. If an ostensible audit were to be conducted on DREs, at best this audit would verify the DREs are functioning in a deterministic manner (benign or malicious) at the moment it is being tested. At worst, if the audit results differ from the original then the machines are not functioning in a deterministic manner and the results of the election cannot be trusted, and, unlike paper ballot elections, such errors cannot be remedied.

6. This inherent design flaw, the lack of a voter verified paper trail, means if there are any flaws in how the paperless DRE records votes, then there is no way to detect or correct any mistakes during a post-election audit.

My experience with Diebold voting machines

7. In my research with Diebold AccuVote TS and TSx machines, (the DRE models used in Georgia) I rely on a wealth of academic research conducted detailing how Diebold voting machines have never been a secure way of recording votes, and have known vulnerabilities which call into question results.

8. Motivated by Kohno et al., TTRB, and EVEREST, (see Bernhard Declaration, *passim*) I have begun writing software to independently verify a selection of vulnerabilities of the Diebold AccuVote voting system detailed in those studies. My focus has been on developing methods to quickly verify that the version of software currently used in Georgia, Ballot Station 4.5.2!, is vulnerable to known attacks identified in the academic research. If 4.5.2! is found to be vulnerable to these select attacks, then

it is highly likely that Georgia's version of software is also vulnerable to other attacks detailed in the academic research.

9. Even without running this software to verify likely vulnerabilities affecting version 4.5.2!, the software should be assumed to have critical vulnerabilities since other version of software including 4.3, 4.6, and 4.7 (released before and after 4.5.2!) have had critical vulnerabilities affecting them.

10. I have written software to decrypt ballot results files for BallotStation 4.3.15 and see how votes were cast in order, violating voters' secret ballot protections. I have also created smart-cards which can record the *Smart Card Key* as detailed in EVEREST report (13.3.7). This is the first step in creating illegitimate supervisor cards and infinite voter cards, permitting an unlimited number of votes to be cast by the voter. This vulnerability almost certainly affects 4.5.2! since it affects versions created before and after the Georgia version. I've also written software which is capable of decrypting the file *bs-security.cf* (EVEREST 13.3.5). EVEREST says this attack, "creates the potential for more serious attacks. For instance, malicious software (i.e., a virus) could use this knowledge to alter election results, erase system logs and/or leak the keys necessary to create fraudulent smart cards (e.g., Voter Cards)."

KSU server findings and implications

11. On August 23, 2016 I went to the Fulton County Elections Department in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conduct a wireless security assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment was at that time managed by the Center for Election Systems at KSU.

12. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the CES public website to see if there were any public documents that could give me background on CES and Merle King's duties. I used the search "site:elections.kennesaw.edu inurl:pdf" at www.google.com and discovered what appeared to be files relating to voter registration cached by google.

13. When a search engine like Google caches a file, the search engine makes a local copy of the file in case the original link to the file becomes unavailable. Google had already made copies of some of these files on the CES server prior to my accessing them. So, even if CES were to rectify the situation and remove the files from its web server, Google would still have a copy, generally making it available to the public without authorization

14. After this discovery, I wrote a quick script (simple program) to download what public files were available from the CES server here: https://elections.kennesaw.edu/sites/ , at the time a publicly accessible site. No passwords or authentication were required to gain access to these sensitive files. After running the script to completion, I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:

a. voter registration databases filled with personally identifiable information of over six million voters (filename *PollData.db3*). The data included driver's license numbers, birthdates, full home addresses, the last four digits of social security numbers, and more.

b. Election Management System GEMs databases (.gbf and .mdb extensions) GEMS is the central tabulator of the voting system, and used to create ballot definitions, program memory cards and tally and store and report all votes when

an election closes. I was able to access and download GEMS databases for at least 15 counties. These GEMS databases use poor encryption, allowing third parties to extract usernames and passwords for multiple databases.

c. Multiple training videos, of particular interest *CES-BulkUpdate_Final.mp4*. This video details how to update the voters' list containing private and personal voter information using a file downloaded over the internet from elections.kennesaw.edu. The video details navigating to elections.kennesaw.edu, logging into the website, downloading *PollDataUpdates.db3*, placing this file on a memory card, inserting that card into an ExpressPoll Unit (the electronic pollbook), and finally applying the absentee update to the ExpressPoll unit. It appears the counties Fulton, Cobb, Dekalb, Gwinnett, Forsyth, Chatham, Muscogee, Henry, Columbia, Clayton, and Cherokee download files from elections.kennesaw.edu and put those files on ExpressPoll units for use in the polling places to validate voters and issue electronic ballots. (I have attached as Exhibits 1 and 2 are collections of documents that I understand were produced by KSU in 2017 in response to an Open Records Act Request. The records referred to in this paragraph appear on Exhibit 1, page 27).

d. PDFs of election day supervisor passwords, for example, *July 2016 Primary and NP Election Runoff Password Memo.pdf*. Supervisor passwords control the administration of the DRE voting machines in the polling place including opening and closing of the voting machines as well as making administrative corrections when machine problems are encountered.

e. Windows executables and DLLs, for example:

- *System.Data.SQLite.DLL*
- *ExpDbCreate.exe*
- *ExpReport.exe*

15. It appears these files are used by the Diebold ExpressPoll (electronic pollbook) units. Since ExpressPoll units are specialized Windows PCs, an attacker can modify theses files and affect the behavior of the ExpressPoll units at the polling place when voters are checked in to vote, assigned a particular ballot style, and approved for voting. A list of vulnerabilities affecting ExpressPoll units is located on the internet at the following URL: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md

16. On August 28, 2016 and August 29, 2016, I contacted King by email and telephone to warn him that CES should assume that the sensitive documents hosted on the "elections.kennesaw.edu" server had already been downloaded by unauthorized persons. Yet for reasons that have never been explained, the server was not secured for months. Along with my colleague Christopher Grayson, I accessed the server again several times in late February 2017 and was able to access and download the same types of files that I had accessed months earlier.

17. Besides making the above information available to the public, the server at elections.kennesaw.edu ("Election Server") was running a version of Drupal, a widely-used content-management framework for websites, which is vulnerable to an exploit called "drupageddon." Using drupageddon, an attacker can compromise a vulnerable server with ease. A public advisory for drupageddon was released in 2014, alerting users that an attack, "can lead to privilege escalation, arbitrary PHP execution, or other

attacks." In practice this means an attacker could have created, modified, or deleted files on the web server, likely without detection.

18. Drupal assigned this vulnerability the highest security risk score possible, 25/25 (Highly Critical).

19. Drupal released a tool to help with the identification of vulnerable servers, called Drupalgeddon (with an L), and made the following critical warning regarding the use of the tool:

> "Drupalgeddon drush command is only useful when restoring from backups is not an option and sufficient expertise is available to attempt a labourious manual recovery. Even then, **neither Drupalgeddon nor an expert can guarantee a website has** not **been compromised.** They can only confirm with certainty that a site *has* been compromised. This is because:
>
> - Drupageddon attacks may not leave any trace at all
> - Attacks that do leave traces change faster than what Drupalgeddon maintainers can keep up with
> - It is impossible to think of all the places that attackers might hide a backdoor.
> - **There are known exploits that Drupalgeddon does not yet check for.** Contributions are welcome (see below).
>
> If you decide to use Drupalgeddon; **Good luck to you; You will need it**."

20. Based on internal CES staff emails obtained in public records, management was fully aware of the severity of these vulnerabilities, noting that elections.kennesaw.edu was identified as having "a number of critical and severe vulnerabilities some of which are reported to be exploitable" in September 2016 and "40+ critical vulnerabilities" in October 2016. (The documents referred to in this paragraph may be found on pages 40 and 34 of Exhibit 2.) The fact that the server was allowed to remain online for months until notified again of vulnerabilities is completely inexcusable in my opinion.

21. It is my opinion that the Diebold DRE-based election system and its components should not be used in a public election. It is my opinion that the system, given the level of exposure it was and is still presented with, must be assumed compromised, which necessitates a thorough scrubbing of every component and reinstallation of vendor's certified software. Even after a thorough scrubbing of every component, without software updates to remedy vulnerabilities the risk of compromise and implantation of malware still remains high.

22. From the training video *CES-BulkUpdate_Final.mp4* and open records, we know files from the internet-accessible website elections.kennesaw.edu, a vulnerable server, are placed on ExpressPoll units. This means an attacker could have had a straightforward attack-chain of remotely compromising elections.kennesaw.edu and implanting malware on files that are placed on ExpressPoll units, directly compromising the purportedly "air-gapped" system. Although this particular server no longer operates in the state's election administrative operation, any malware that may have been introduced during periods of security failure would very likely still be present on ExpressPoll books or on the other voting system components which remain in use across the state.

23. The system is flawed by design and made worse by the KSU exposure in ways that cannot be practically mitigated. The system should be treated as untrustworthy for the conduct of Georgia's elections.

Poor Physical Security Affecting Voting Systems

24. I have visited the Fulton County Election Preparation Center on multiple occasions, and have been able to freely roam the facility at times. While observing public

logic and accuracy pre-election testing of voting machines with colleagues, on one such visit I noted:

a. A stack of unsecured supervisor cards, which operate the DRE voting machines;

b. Multiple unsecured voter access cards, which are used by voters to activate their electronic ballot on the DRE;

c. A box of unsecured DRE memory cards;

d. A paper printout of a supervisor password;

e. Multiple unsecured Accuvote TS machines with the hinged door which protects the memory card slot unlocked. (These machines were also powered on. An attacker could have easily inserted a malicious smart card or memory card into these machines.); and

f. The cameras on the interior of the building do not have full view of the facility, an attacker can easily gain access to machines while out of view of the cameras.

An attacker could have easily stolen or modified the various unsecured pieces of election hardware.

25. On July 24th, 2018 my colleagues and I observed the closing of the polls at Grady High School. After the polls were closed, my colleagues and I were left unattended for the evening with the voting machines in the school gymnasium. The only measures taken to secure these voting machines were:

a. A cable lock binding all the voting machines together;

b. Tamper evident seals on the machines; and

c. A single security camera.

26. An attacker could have easily disabled the security camera and then modified or stolen the voting machines. The machines were secured with tamper evident seals which can be purchased on the internet at the following URL: http://www.intab.net/Large-Pull-Tite-Seals/productinfo/03-1330/003%20BLUE/

Summary

27. Based on my personal observations, research and knowledge of the authoritative academic studies, it is my opinion that the use of the Diebold DRE voting machines should be immediately curtailed, and not permitted for use in Georgia's elections. Remaining components of the Diebold DRE-based voting system such as the GEMS server, AccuVote optical scanners, and the ExpressVote electronic pollbooks must undergo decontamination procedures prior to use in future elections.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 3, 2018.

Logan Lamb

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

SUPPLEMENTAL DECLARATION OF LOGAN LAMB

LOGAN LAMB declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

Background and Credentials

1. My name is Logan Lamb. I am a cybersecurity researcher based in Santa Monica, California.
2. I have a Bachelor of Science and Master of Science degrees in computer engineering from University of Tennessee, Knoxville.
3. I have worked professionally in cybersecurity since 2010 when I started at Oak Ridge National Lab in the Cyber and Information Security Research group. In that position, I specialized in static and symbolic analysis of binaries, red-teaming prototype critical infrastructure, and de-identifying geospacial data.

4. I now work for the micromobility company Bird as a Senior Vehicle Security Engineer. In this role I protect Bird's fleet from both hardware and software-based hacking attempts.

5. I hereby incorporate my previous declaration as if fully stated herein. (Dock. 258, p. 126) In summary, in August 2016 I discovered serious vulnerabilities affecting elections.kennesaw.edu. The website was misconfigured so that it leaked confidential election data and the version of its content management system, Drupal, was out of date and vulnerable to a well-known exploit called drupageddon. An announcement from the Drupal security team on October 29, 2014 details how severe this vulnerability is, stating that if a vulnerable Drupal server was not updated within 7 hours of the announcement it should be assumed compromised. The Drupal software was still vulnerable in August 2016.[1]

6. Despite these warnings, KSU continued running the vulnerable version of Drupal until August, 2016, almost two years after patches were made available.

7. The server running elections.kennesaw.edu was taken offline on March 2nd, 2017 after KSU was notified a second time the server was still leaking sensitive election data. A forensic image of this server was created on March 6th, 2017 by the FBI.

8. The forensic image created by the FBI was provided to me in late December 2019 by CGG after I signed the protective order. After receiving a copy of the forensic image I confirmed the image was an exact copy of the one created by the FBI by comparing the SHA1 hash of the image to that provided to me.

[1] https://www.drupal.org/PSA-2014-003

9. On January 1, 2020 I began conducting a forensic audit of the provided image of the server running elections.kenessaw.edu.

10. The server image appears to contain all the files, databases, logs, and programs that were saved on the server when it was copied by the FBI on March 6th, 2017.

11. From my initial review of the server, I have four novel findings so far:

    a. There is evidence which suggests the server was compromised in December, 2014, well before the 2016 election.

    b. Access logs which would be critical to forensic work only go back to November 10, 2016, two days after the 2016 election.

    c. Election related files were deleted on March 2nd prior to taking the server offline and prior to the FBI creating an image.

    d. The version of BallotStation used by Georgia, 4.5.2!, is likely vulnerable to exploits affecting BallotStation 4.3.15 and beyond. Critical exploits affecting version 4.3.15 were documented in 2006.[2]

12. In the following sections I will expand on the above findings.

INDICATORS OF COMPROMISE

13. I found evidence which suggests a well-known attack named "shellshock" was successfully used against the server. The attack exploits a bug in common server software and gives the attacker full control of the computer. The Shellshock bug was so widespread, easy to exploit, and potentially devastating that when it was discovered in

[2] https://s3.amazonaws.com/citpsite/wp-content/uploads/2019/01/23191614/ts06full.pdf

September of 2014 it received significant media attention and dire warnings from the Department of Homeland Security.[3]

14. Despite those warning, CES did not patch the bug for months.

15. On December 2, 2014, while the KSU server remained vulnerable, a new user named "shellshock" was created on the server. I have created the below timeline of activity related to the shellshock user after fusing logging data from multiple sources. The timeline may not be complete:

16. 12/2/2014 10:45 – the user mpearso9 is modified using the Webmin console

    12/2/2014 10:47 - shellshock user created using Webmin console

    12/2/2014 10:49 - /home/shellshock/.bash_history last modified

    12/2/2014 11:02 - /home/shellshock/shellsh0ck file is deleted

    12/2/2014 11:06 - bash patched to version 4.2+dfsg-0.1+deb7u3 to prevent shellshock

    12/2/2014 11:40 - shellshock user disabled using Webmin console

17. The file named ".bash_history" is a kind of log that typically records all the commands a user executes. For this user, though, the file contained a single command to logout of the server. The single command to logout is suspicious since a file was created and deleted in the user's home directory, leading me to believe the ".bash_history" has been modified. This indicates to me that the "shellshock" user may have been hiding their activities.

18. When an attacker breaks into a server, it is common that they fix the bug that gave them access. That way, the attacker can keep control while keeping other would-be attackers out. That appears to be what happened on the KSU server. Just 20 minutes after the "shellshock" user was created, the logs show that the shellshock bug was patched.

[3] For a contemporary report, see https://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html

19. The long unpatched software, unusual username, potentially modified command history, and near immediate patching of the shellshock bug are all strong pieces of evidence that an outside attacker gained access to the KSU server by exploiting the shellshock bug. There may still be other explanations. It is possible, for example, that a CES employee used a convoluted method of patching shellshock on December 2nd, 2014. Additional forensics need to be done to confirm the attack and determine what the attacker may have done with their access to the server.

20. If an attacker did indeed exploit the shellshock bug, then they would have had almost total control of the server including the abilities to modify files, delete data, and install malware.

MISSING LOGS

21. The website software, Drupal, was configured to maintain an access log. The access log contains all requests made to the webserver. If an attacker attempted to exploit drupageddon on the webserver then it would be apparent in the access log. However, the access log records on the server only go back to November 10, 2016, two days after the 2016 election.

22. The access logs will retain information indefinitely unless configured to automatically delete the oldest records based on age.

23. The missing logs could be vital to determining if the server was illegally accessed before the election, and I can think of no legitimate reason why records from that critical period of time should have been deleted.

FILES DELETED PRIOR TO FBI HANDOFF

24. In addition to the missing logs, there are also scores of files deleted on March 2nd, 2017. Some of the files appear to be unusually deleted and directly related to elections. Using the software "TestDisk,"[4] I was able to do a forensic search of the server image to find deleted files. I found many files deleted on March 2nd, 2017, just before the server was taken offline by the CES/KSU staff and the original server handed over to the FBI. I have not yet been able to determine what these deleted files were, but include the filenames below which I believe are related to elections and were deleted on March 2nd, 2017.:

2-Mar-2017 12:15 /countyfolders/Appling County/ExpressPoll/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/Appling County/ExpressPoll/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/Appling County/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/Appling County/Proof/Ballots/1-90-NP-FB.pdf

2-Mar-2017 12:15 /countyfolders/do_not_use.php

2-Mar-2017 12:15 /countyfolders/do_not_use.php

2-Mar-2017 12:15 /countyfolders/Murray County/Proof/Audio/Murray Audio.zip

2-Mar-2017 12:15 /countyfolders/Murray County/Proof/Audio/Murray Audio.zip

GEORGIA MACHINES VULNERABLE TO KNOWN ATTACKS

25. In the server image I found three files which indicate the DREs in Georgia running BallotStation 4.5.2! are vulnerable to exploits affecting BallotStation 4.3.15:

    a. explorer.glb – this file is used as a backdoor to log into Windows CE on a DRE

[4] https://www.cgsecurity.org/wiki/TestDisk

b. BS_CE-TSR6-4-5-2!-DS.ins – a script which installs BallotStation on an Accuvote TS

c. BS_CE-TSX-4-5-2!-DS.ins – a script which installs BallotStation on an Accuvote TSX

26. I was able to extract BallotStation.exe from BS_CE-TSX-4-5-2!-DS.ins and confirm the DES key **F2654hD4** is in it. Because this encryption key has been publicly known for years, it means that anyone with access could have decrypted and altered data the DREs were meant to protect. That is, any encryption done by the DREs could have been trivially undone, and that important layer of security would have been totally ineffective.

27. The inclusion of this DES key indicates Georgia's version of BallotStation is likely very similar to version 4.3.15 which was extremely vulnerable to compromise. Like all the other data on the server, it was poorly secured could have been tampered with.

OTHER BAD PRACTICES

28. According to Michael Barnes' testimony, the server was supposed to be used for a few limited purposes. In reality, it appears elections.kennesaw.edu was the primary server for CES and was used for a wide variety of purposes. It includes copies of BallotStation to be installed on the DREs; databases of pollbook data for every registered voter in the state, including personally identifiable information; GEMS database files for numerous Georgia elections; training materials, and related machine and file passwords. The server even had installer files for Adobe Photoshop. A cursory review of these other files saved on the server show some other bad cybersecurity practices putting components and election files across the state at risk of intrusion and compromise.

29. The election and business files on this potentially compromised server appear to be of the type transferred between various parts of the State's election infrastructure over many years. As Dr. Halderman stated in his Declaration, "Although the KSU server itself was decommissioned in 2017, many of these potentially infected computers likely remain in use with the BMD-based system." (Doc . 692-3 ¶4). I agree with his conclusion.
30. It is unreasonable to assume that the new BMD election system and supporting infrastructure is not already potentially compromised or exposed to malware or given the broad range of election files on the CES elections.kennesaw.edu server.
31. Forensic analysis of the DRE components should be conducted to fully understand the nature of potential past compromises and to properly assess the current and future threat to the BMD system components and the systems that feed it, like the voter registration system.

I declare under penalty of perjury that the foregoing is true and correct and that this declaration was executed this 14th day of January, 2020.

LOGAN LAMB

EXHIBIT D

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRAD RAFFENSPERGER, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF KEVIN SKOGLUND

KEVIN K. SKOGLUND hereby declares under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I have personal knowledge of all facts stated in this declaration, and if called to testify, I could and would testify competently thereto.

Background and Qualifications

2. My name is Kevin Skoglund. I reside in the Commonwealth of Pennsylvania. I hold a Bachelor of Arts degree from Harvard University.
3. Since 2003, I have owned and operated Nova Fabrica, a company which engages in software programming, web development, digital security consulting, and training.

4. I have taught over 30 online courses for LinkedIn Learning, including several courses focused on digital security: “Programming Foundations: Web Security,” “Web Security: User Authentication and Access Control,” and “SSL Certificates for Web Developers.”
5. I cofounded Citizens for Better Elections, a nonpartisan grassroots group advocating for resilient, evidence-based elections. I currently serve as the Chief Technologist.
6. I am the Senior Technical Advisor to the National Election Defense Coalition (NEDC). NEDC is a national organization working to secure elections technology by bring together experts in cybersecurity and elections administration, policymakers, NGOs, and concerned citizens to build bipartisan consensus on a comprehensive, cost-effective plan to secure the vote.
7. Since May 2017, I have been an active participant in the National Institute of Science and Technology (NIST) Voting System CyberSecurity Working Group. The purpose of the group is to provide security guidance for voting systems to inform the development of the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG). For over two years, the CyberSecurity Working Group has been developing security guidelines and requirements for the next generation of voting systems.

8. I am one of the leaders of an election security group which identified and continues to track election systems connected to the internet, as reported in the Vice article, "Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," on August 8, 2019.[1]

9. I have engaged in coordinated disclosures of vulnerabilities in election systems with the EAC, the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the Department of Homeland Security (DHS), state governments, and voting system vendors.

10. I have written several online articles, listed below, about electronic ballot marking devices generating barcodes on ballots and how barcodes could be modified to represent new values.

    i. Deconstructing an ES&S ExpressVote Paper Record[2]

    ii. How the ExpressVote XL Could Alter Ballots[3]

    iii. How ExpressVote Barcodes Could Be Modified[4]

11. I collaborated with the University of Pittsburgh Institute for Cyber Law, Policy, and Security to conduct an analysis of voting system purchases

---

[1] https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

[2] https://securiosa.com/posts/deconstructing_expressvote_records.html

[3] https://securiosa.com/posts/how_the_expressvote_xl_could_alter_ballots.html

[4] https://securiosa.com/posts/how_expressvote_barcodes_could_be_modified.html

across Pennsylvania's 67 counties.[5] Among our principal findings, we show that the average cost of voting systems where most voters machine-mark ballots was $24.20 per registered voter, while the average cost of systems which rely primarily on hand-marked paper ballots was $12.18 per registered voter, half the cost.

12. I serve as a Judge of Election in Montgomery County, Pennsylvania. The polling place I oversee uses a voting system manufactured by Dominion Voting Systems, Inc. ("Dominion"), configured so that most voters hand-mark a paper ballot and voters who want assistance use a ballot-marking device ("BMD"). The hardware and software is similar to the system being proposed for use in Georgia, but configured differently.

Proposed Voting System for the State of Georgia

13. It is my understanding that the State of Georgia is planning to adopt a paper-based voting system ("Georgia's Dominion Voting System") manufactured by Dominion, and intends for most voters to use an ImageCast X touchscreen computer configured as a BMD ("Dominion BMD") to create a ballot and to use an ImageCast Precinct optical scanner ("Dominion op-scan") to scan and to tabulate the ballot. This polling place configuration is often referred to as a "BMDs for all voters" style of voting ("BMDs-for-All").

[5] https://www.cyber.pitt.edu/votingsystemsanalysis

14. It is my understanding that the State of Georgia is planning to adopt a system of electronic pollbooks ("Georgia's KNOWiNK Pollbook System") manufactured by KNOWiNK, LLC ("KNOWiNK"), and intends for all polling places to have Poll Pads ("Poll Pads") to determine the eligibility of voters and to sign them in prior to voting.

15. I have read the declaration of J. Alex Halderman filed on October 4, 2019, and I concur with all of the facts, expert opinions, and conclusions stated therein.

16. I have read the declaration of Philip B. Stark dated October 22, 2019, and I concur with all of the facts, expert opinions, and conclusions stated therein.

17. It is my opinion that Georgia's Dominion Voting System raises significant election security and integrity concerns. It would unnecessarily add risks which could prevent accurate election results from being generated, and cause irregularities and malfunctions to go undetected.

Availability and Resilience

18. The primary concern of BMDs-for-All is that a well-functioning computer becomes a prerequisite for marking a ballot and introduces a risk that it will be misconfigured, malfunction, or otherwise not be available.

19. "Resilience" is an important property of secure systems. Resilience is the ability of a system to deliver the intended functionality continuously, to manage any problem and to recover from it with minimal impact.

20. There are real-world examples where voting systems were not resilient. Voting machines failed to start, malfunctioned during an election, or lost power. There are examples where short-term risk-mitigation measures, such as backup power supplies and emergency/provisional paper ballots, failed or were exhausted.

21. The unavailability of data resources is referred to as a "Denial of Service" ("DoS"). If all BMDs in a polling place are inoperable it would result in a complete Denial of Service, likely resulting in turning away voters. If some BMDs are inoperable or intermittently malfunctioning it would result in a partial Denial of Service, likely resulting in longer or slower-moving lines to vote.

22. Long lines to vote are a security concern because they reduce the availability of the voting system to all voters who wish to use it. Long lines may discourage voters from casting a ballot and can be an intentional or unintentional form of voter suppression.

23. BMDs-for-All inherently causes longer and slower-moving lines compared to systems in which most voters hand-mark paper ballots, because the voting capacity of each polling place is limited to the number

of BMDs deployed and each voter has exclusive use of a BMD while making their selections, which can be a time-intensive task. Systems with hand-marked paper ballots do not have a similar bottleneck because many voters can mark their selections in parallel.

24. BMDs-for-All is not resilient to the risk of long lines because there is no easy way to increase voting capacity, due to the fact that a BMD is a prerequisite for marking a ballot. Systems with hand-marked paper ballots can easily add more voting capacity by adding cardboard privacy screens or passing out clipboards.

Susceptibility to Errors

25. All BMDs incorporating touchscreen interfaces are vulnerable to errors due to touchscreen miscalibration. A voter may touch a preferred candidate and their vote will either not register or register for a different candidate ("vote flipping"). Touchscreen miscalibration errors decrease usability, reduce public trust in the election, and diminish overall confidence that voter intent is being captured accurately.

26. All BMDs are vulnerable to malfunction when printing a ballot. The printer may malfunction, run out of consumable supplies, or fail to print the entirety of the ballot.

27. All BMDs are vulnerable to Presentation Attacks, where the voter makes one selection but the BMD outputs a different selection on the paper

record. The success of a Presentation Attack depends on the voter not noticing the change and submitting the modified vote. Post-election audits will be unable to detect the discrepancy. The BMDs most vulnerable to Presentation Attacks are those with impediments to voter verification.

Concerns about Voter Verification

28. All BMDs require an addition verification action by voters to check that the BMD has marked the ballot correctly in order to ensure that a ballot to be cast was accurately marked by the machine. Checking the work of a computer should not be required of a voter and is not required when hand-marking a paper ballot.

29. While BMDs produce evidence of every vote, they produce weak evidence. Our judicial system is familiar with the notion that all evidence does not carry equal weight. BMD-generated ballots are only as strong as a voter's willingness and ability to verify the paper record for errors and to take effective action on any errors they find.

30. Several studies have shown that a significant number of voters do not verify machine-generated ballots carefully and do not detect errors.[6]

---

[6] Rice University: https://www.usenix.org/system/files/jets/issues/jets-0101-greene.pdf
Georgia Institute of Technology: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3292208

31. In "Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters,"[7] the authors—Andrew Appel, Richard DeMillo, Philip Stark—enumerate the many obstacles to reliable voter verification of machine-marked ballots. They explain that risk-limiting audits ("RLAs"), designed to limit the risk of an incorrect outcome, are incapable of limiting the risks introduced by BMDs-for-All. I concur with their analysis.

Problems with Ballot Summaries

32. Dominion BMDs use commercial off-the-shelf (COTS) printers to print a ballot on blank paper stock which contains a two-dimensional barcode ("QR code") and a summary of the voter's ballot choices ("ballot summary").

33. Dominion BMDs print ballot summaries with an abbreviated label for some contests. For example, I possess a sample ballot labeling a contest as "County Unified Gov Brd Mem". The contest labels appear to have a maximum length which requires truncation. Such abbreviations inhibit the ability of voters to verify that their selections are listed correctly.

34. Dominion BMDs do not print the full text of any ballot proposition or question and these types of contests are routinely assigned a cryptic contest label instead. In the 2017 general election in Denver, Colorado, a

[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755

Dominion BMD labeled eight long and complex ballot questions[8] in the ballot summary as "Referred Question 2A" through "Referred Question 2H," and "Initiated Ordinance 300."[9] (See Attachment B.) No voter can be expected to reliably remember what issues are being referenced by these labels. The voter selections listed are also difficult to decipher and are adverse to voter verification: "Vote for YES/FOR - SI/EN FAVOR DE."

35. Dominion BMDs print ballot summaries which indicate when a voter does not make a selection in a contest, however they do not indicate if *both* the contest and the selection has been omitted, due to malfunction or malfeasance. To detect this problem, each voter would have to remember all contests presented on the touchscreen and notice that a contest was not included in the printed list.

36. My experience with the Dominion BMD is that, when voters increase the size of the text on the screen to improve readability, the size of the text printed for the ballot summary, used for voter review, will not similarly increase. The text remains in the default font set for the election, which is typically a 10pt sans-serif font. Text which is small or whose size is not

---

[8] The full text of the ballot questions can be reviewed at https://ballotpedia.org/November_7,_2017_ballot_measures_in_Colorado

[9] See Attachment B,

under voter control inhibits the ability of voters to verify that their selections are listed correctly.

37. Even if voters are willing to take the time to attempt to verify the human-readable text in the ballot summary and make their best efforts to be accurate, there is no way to know whether their "verification" was accurate. Those administering the election cannot know if any voter, and therefore certainly not every voter, attempted to verify or did so successfully. As a result, ballots which use ballot summaries cannot be viewed as a reliable source record for auditing.

Problems with Barcodes

38. Barcodes increase the reliance on available, well-functioning BMDs in order to conduct an election. A BMD is a prerequisite for casting a ballot because a voter cannot create a barcode without its assistance.

39. Barcodes are machine-readable, but not human-readable. A device—such as a computer, barcode scanner, or smartphone application—is necessary to read the data stored in a barcode.

40. The Dominion BMD encodes vote selections inside one or more QR Codes as an alpha-numeric string of characters. This string of characters only has meaning to the voting system. It is proprietary. Any interpretation of the data stored in QR codes, even during post-election audits, is dependent on the voting system.

41. The QR codes may contain more than ballot selections. They could contain metadata associated with the ballot which can be used to determine the identity of the voter or the order in which votes were cast. Metadata which can be used to identify voters has been observed in the barcodes of other voting systems. The data stored in barcodes is unregulated and is not examined during federal certification.

42. The QR codes are not voter-verifiable. Even with a device to assist them, voters are unable to verify that the QR codes contain the correct information to ensure that their ballots are being cast-as-intended. A voter requires transparent information to make the choice to cast or to reject a machine-marked ballot. If a voter cannot read the data that will be cast and sent to the tabulator, then a voter cannot make an informed choice.

43. Barcodes are the only votes that are tabulated by the op-scan. The election results are the aggregate of the barcodes counted.

44. A voter can only verify the portion of the paper record which is human-readable text. The Dominion op-scan does not interpret or tabulate the contents of the human-readable text in the ballot summary. In contrast, another EAC-certified voting system, the Hart Verity Duo, does not use barcodes to store vote selections and uses optical character recognition ("OCR") to tabulate the human-readable text in the ballot summary.

45. The human-readable text in the ballot summary will only be inspected by officials if there is a manual recount or audit which includes such inspection and if the ballot is selected for review. The ballot summary serves as a voter-verifiable paper audit trail ("VVPAT").

46. Voting systems with barcodes and ballot summaries are vulnerable to Barcode/VVPAT Mismatch Attacks ("Mismatch Attack"), where a BMD outputs the correct selections in the ballot summary but encodes different selections in the barcode. The voter cannot notice the modified votes and will approve the ballot.

47. A barcode and ballot summary may not match for reasons unrelated to malicious attacks. As an example, in the 2016 Maryland General Election, a BMD printed barcodes for 18 contests but only printed the human-readable text for three. The voter still cast the ballot and the barcodes were counted, but the human-readable text is not auditable.[10]

48. Barcodes provide a path for hacking a voting system which does not exist with a ballot without barcodes. A barcode scanner can be thought of as a keyboard, which can submit any input when a barcode is read by the voting system. It may be possible to send commands which exit the running the voting system program. It may be possible to send commands

[10] See Attachment A, from Maryland Board of Elections slideshow, slide 27, accessible at http://www.ncsl.org/Portals/1/Documents/Elections/Elections_June2017_Ballot_Image_Audits.pdf

which allow a code injection, which can cause arbitrary code to be executed.

Concerns about Electronic Pollbooks

49. As with the voting system, the primary security concern of electronic pollbooks is that a well-functioning computer becomes a prerequisite for determining a voter's eligibility and introduces a risk that it will be misconfigured, malfunction, or otherwise not be available.

50. There are real-world examples where electronic pollbooks have malfunctioned, resulting in confusion, long lines, or voters being turned away. Problems may have allowed voters to vote more than once.[11]

51. The best practice to ensure that voter check-in is resilient to problems is to have paper pollbooks as a back up in every polling place. The paper pollbooks must be up-to-date with the current voter registration database and must be reconciled or updated after the early voting period to ensure that early voters are ineligible to vote a second time.

52. Poll Pads include networking capabilities over WiFi, cellular modem, and Bluetooth. Poll Pads use WiFi or cellular modem to connect to a central server hosting the election registration management software. Poll

---

[11] Johnson County, IN: https://www.in.gov/sos/elections/files/Report%20-%20Johnson%20County%20ePB%20Investigation%20Dec%2031%202018.pdf
Durham County, NC: https://www.charlotteobserver.com/news/local/article113248708.html
Lehigh County, PA: https://www.mcall.com/news/elections/mc-nws-lehigh-county-vote-twice-opportunity-20181109-story.html

Pads use Bluetooth to share voter check-in data with other Poll Pads in the same polling place to prevent double-voting. The Poll Pad can still function (with reduced features) if some or all of these network services are disabled.

53. Running any network services increases the risk of cyberattack, either through unauthorized connections to the system or using Machine-in-the-Middle Attacks where a malicious actor either intercepts, modifies, or eavesdrops on network communications. If network-based features are not essential, networking services should be disabled.

54. I am aware that in June 2019, the City of Philadelphia purchased 3,550 KNOWiNK Poll Pads for $2.7 million and planned to use them for the first time in November 2019. In August 2019, Stephanie Tipton, the city's acting chief administrative officer, notified the Board of Elections that they had encountered problems. She wrote: "The observed problems included failures to properly connect to voting machine printers and inadequate election night reporting." The project management team recommended against using the Poll Pads because "it does not have confidence that KNOWiNK's poll book system will be able to perform reliably for this November's election."[12]

[12] https://www.inquirer.com/politics/philadelphia/philly-epollbook-electronic-systems-should-not-be-used-city-says-20190917.html

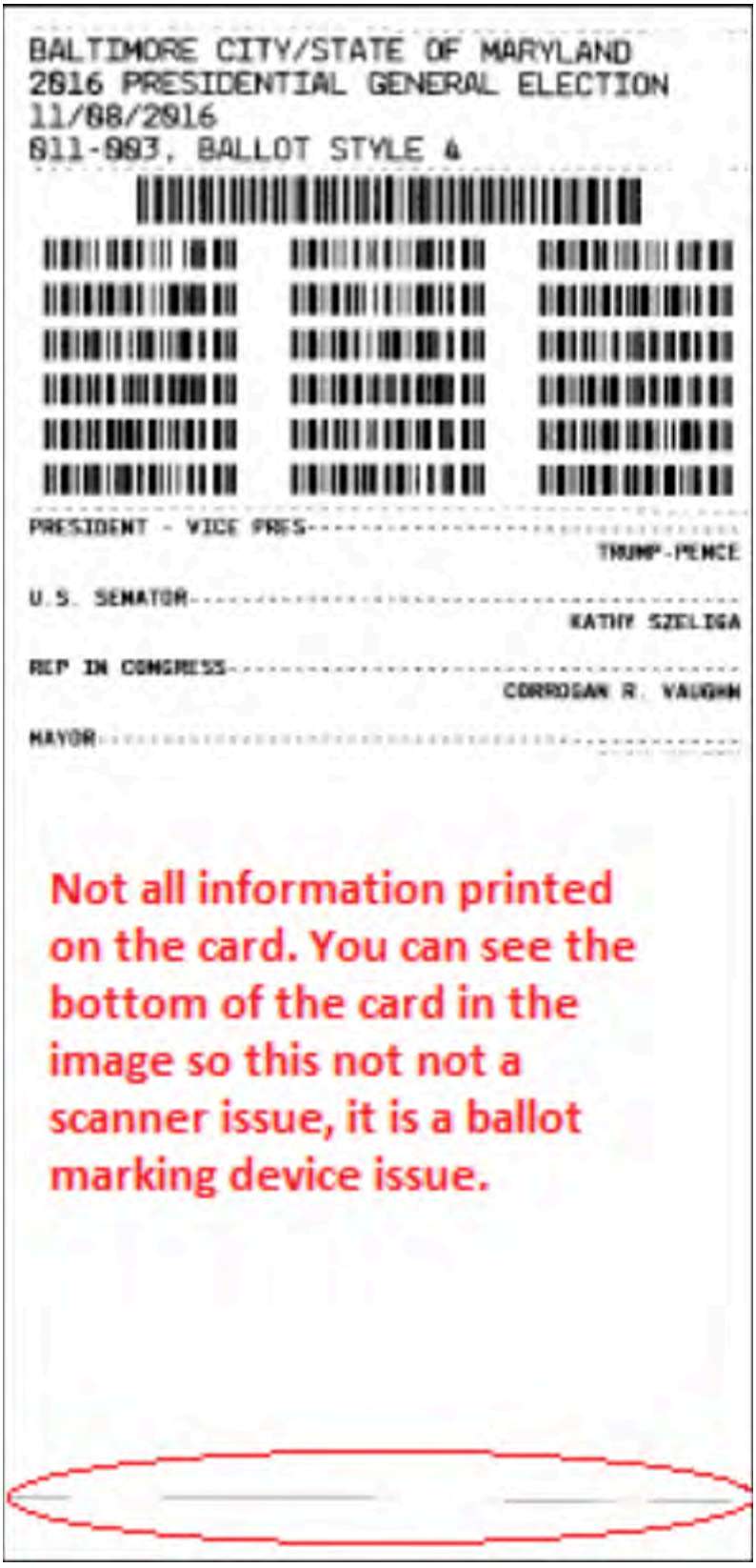
55. Unlike voting systems, the EAC does not certify electronic pollbooks, nor does it review their functionality or security. The responsibility falls to each state to independently review the functionality and security of electronic pollbooks.

56. A thorough cybersecurity review of the Poll Pad installation in the polling place should be conducted, primarily to ensure that unauthorized access to the Poll Pad and to the voter database is prevented.

This 22nd day of October, 2019.

Kevin K. Skoglund

Attachment A


BALTIMORE CITY/STATE OF MARYLAND
2016 PRESIDENTIAL GENERAL ELECTION
11/08/2016
011-003, BALLOT STYLE 4
PRESIDENT - VICE PRES
TRUMP-PENCE
U.S. SENATOR
KATHY SZELIGA
REP IN CONGRESS
CORROGAN R. VAUGHN
MAYOR
Not all information printed on the card. You can see the bottom of the card in the image so this not not a scanner issue, it is a ballot marking device issue.

Attachment B

Official Ballot
City and County of Denver
Coordinated Election
Tuesday, November 7, 2017

Boleta Oficial
Ciudad y Condado de Denver
Elección Coordinada
Martes 7 de noviembre de 2017

Ballot 5 - Type 5

1330816830

1489, 149

Director at Large
Vote for Robert Russell Speth

Director District 4
BLANK CONTEST

Referred Question 2A
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2B
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2C
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2D
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2E
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2F
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2G
Vote for YES/FOR - SI/EN FAVOR DE

Referred Question 2H
Vote for YES/FOR - SI/EN FAVOR DE

Initiated Ordinance 300
Vote for YES/FOR - SI/EN FAVOR DE

IMP4-004389

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRAD RAFFENSPERGER, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

SUPPLEMENTAL DECLARATION OF KEVIN SKOGLUND

KEVIN SKOGLUND declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of all facts stated in this declaration, and if called to testify, I could and would testify competently thereto.
2. I attended the court's audio hearing on September 28, 2020 to review the State's plans to make software changes to the ImageCast X ("ICX").
3. Mr. Tyson and Dr. Coomer explained that logic and accuracy ("L&A") testing had revealed a problem: the current ICX software is unable to reliably render the screen for a contest with 30 candidates in two columns of 15.

4. This revelation highlights the importance of robust L&A testing. The State described a rendering problem which manifests under some circumstances and not others. Georgia's voters are lucky it was caught this time. Performing less than the comprehensive testing prescribed in Georgia statue could have allowed this problem to slip through undetected.
5. Dominion has proposed changing the ICX software so that the desired two-column layout will render reliably. Dominion submitted the change to the ICX software to Pro V&V for review. I heard Dr. Coomer express optimism that Pro V&V will endorse the change as "de minimis" later this week.
6. It concerns me that a significant software change is happening at this late date and that pressure to prepare over 30,000 ballot marking devices for this election may result in less thorough review and testing of the proposed change.
7. I have not heard Dominion or the State say that the change to the ICX software has been submitted to the U.S. Election Assistance Commission ("EAC"), or that the EAC had been contacted about the change. It is not uncommon to engage a Voting System Test Lab ("VSTL") to review a change before notifying the EAC. However, the VSTL review is only the

first step in the approval process. Since time is of the essence, I expected the EAC would be included at the earliest stages.

8. The EAC's Testing and Certification Program Manual describes the procedure for a de minimis change. It introduces them with: "A proposed de minimis change may not be implemented as such until it has been approved in writing by the EAC."[1]
9. After a VSTL reviews the proposed change, "[t]he EAC will review all proposed de minimis changes endorsed by a VSTL. The EAC has sole authority to determine whether any VSTL endorsed change constitutes a de minimis change under this section. The EAC will inform the Manufacturer and VSTL of its determination in writing."[2]
10. The federal certification of a voting system is voided if the software is modified prior to the EAC's written determination. ("Any modification to the system not authorized by the EAC will void the certificate."[3])
11. The certification guidelines are strict in order to safeguard the integrity of the voting system.
12. It is not certain if the EAC will approve the proposed change to the ICX software as a de minimis change.

---

[1] "Testing and Certification Program Manual," Section 3.4.3, available at: https://www.eac.gov/sites/default/files/eac_assets/1/6/Cert_Manual_7_8_15_FINAL.pdf

[2] "Testing and Certification Program Manual," Section 3.4.3

[3] "Testing and Certification Program Manual," Section 5.11

13. The EAC only began allowing *any* software changes to be considered de minimis on November 15, 2019.[4] Prior to that date, software changes which required a new build of the software and VSTL testing were classified as "system modifications" and subjected to more thorough testing.

14. I have heard EAC staff say the reason for the previous prohibition was the recognition that even a small software change can create unintended consequences that alter the system's reliability, functionality, capability, or operation.

15. I described in my testimony a real-world example which illustrates the wisdom of this approach. It bears striking similarities to the current situation.

16. In November 2019, Northampton County, Pennsylvania wanted to change how candidates were displayed on the touchscreen (of a different brand of voting system) in order to reduce voter confusion. They added some text in the square to the right of some candidates: "Straight Party Vote will light up to the left for this candidate." It seems like a harmless change, but it had a nasty side effect on election day. The votes cast for some candidates stopped being recorded altogether. It was perplexing

[4] "Notice of Clarification 19-01: Software De Minimis Changes," available at: https://www.eac.gov/sites/default/files/voting_equipment/NOC19.01_SoftwareDeMinimisChanges_11-15-2019.pdf

because the affected candidates were not necessarily near any added text and other voting machines used the same data without incident.[5]

17. Small changes can cause large, unintended consequences. Their impact is easy to underestimate.

18. Today, I was surprised to hear Mr. Tyson express the opinion that Georgia law ceases to require federal certification after procuring a new voting system.

19. If the federal certification can in fact be voided on the day after purchase, it undermines all of the excellent reasons to require it in the first place.

20. I am alarmed that any state would contemplate abandoning compliance with the federal standards. I view it as irresponsible and counterproductive. It would put Georgia far outside the norm.

21. The federal standards are a *minimum* set of requirements for any voting system. They are the *starting point* for providing reliable, secure elections. Many states—notably California, Colorado, New York, and Pennsylvania—have rigorous state requirements for security and usability in addition to the baseline federal certification.

22. Voiding the federal certification would void the guarantees that a voting system will meet established minimum standards set by experts for

---

[5] "A Pennsylvania County's Election Day Nightmare Underscores Voting Machine Concerns," *The New York Times*, November 30, 2019, available at: https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html

security, accessibility, usability, reliability, and accuracy. Instead, the voting systems's "guarantees" would be based on an ephemeral, patchwork, of subjective processes that reduce trust.

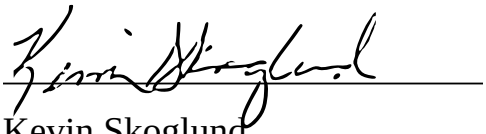
23. Without the nominal standard, Georgia's new voting system can only be as secure and reliable as the less rigorous standard that takes its place.

24. I fear that if the State is motivated to abandon the minimum standards by time pressure or by inconvenience, then the stresses of future elections will motivate the State to cut additional corners.

25. The federal certification of the voting system and its requirements for managing changes provide essential guardrails. They reduce the risks of significant, unexpected problems on election day. It is important to preserve and follow them.

26. My previous declaration and testimony (under seal) underscores my current concerns.

Executed on this date, September 29, 2020.



Kevin Skoglund

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRAD RAFFENSPERGER, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

SUPPLEMENTAL DECLARATION OF KEVIN SKOGLUND

KEVIN SKOGLUND declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of all facts stated in this declaration, and if called to testify, I could and would testify competently thereto.
2. I have read the Letter Report regarding "Dominion Voting Systems ICX Version 5.5.10.32" from Pro V&V to Michael Barnes dated October 2, 2020 ("Letter Report").
3. The Letter Report describes Pro V&V's evaluation of a proposed code change by Dominion to address a flaw in the current ICX software related to reliably displaying two columns of candidates.

4. Pro V&V's evaluation is inadequate to verify Dominion's opinion of the root cause of the error, Dominion's proposed fix for the error, or whether the nature of the proposed change is considered "de minimis" as defined by the U.S. Election Assistance Commission ("EAC").

High Impact Changes

5. The Letter Report describes changes that are potentially high impact.
6. I expected the change to be limited to one or two lines in a configuration file based its description in the hearings. A configuration file change would provide a new value for the existing code to use.
7. The impact of changing a value being *used* by code is far less than the impact of changing the code *itself*, in the same way that changing the furniture in a house has less impact than moving walls. The value may be different but it will travel the same pathways through the code during operation. The structure and governing rules are unchanged.
8. Instead, the Letter Report describes two sets of changes to the source code *itself* in a total of five files. It does not quantify the number of lines changed, but it must be at least five. These are not merely configuration changes. Variable and function definitions in the source code are changed.

9. The changes described may sound minor, for example changing a variable from an integer (e.g., 123) to a string (e.g., “123”), but I would give them no less consideration. I have broken plenty of code making similar changes.

10. One reason is that any code elsewhere in the program that uses a changed variable or function could be impacted. Another part of the code may act correctly when given 123 but act incorrectly when given “123”. The first can have numbers added and subtracted, while the second can be searched for a specific character, but the reverse is often not true.

11. The Letter Report describes a source code review limited to the changed lines of source code. The code comparison performed is similar to reviewing the changed text in a legal blackline. It does not appear that Pro V&V looked throughout the source code for other interactions which could prove problematic.

12. The Letter Report states that Dominion believes the problem is a collision of resource identifiers between their software and the underlying operating system. I think it’s a fair analogy to say that Dominion’s software and the operating system sometimes try to park in the same parking space.

13. In my experience, an abundance of caution is necessary when the operating system and software running on it are working in a shared

space and not playing well together. A misstep could create additional problems in their interactions and any change should be carefully considered and well tested.

14. The Letter Report does not describe any review of the proposed software's interaction with the operating system. It does not mention the involvement of any expert on the operating system or an opinion regarding colliding resource identifiers—the reported cause and the target of the resolution. This is a concerning oversight.

Inadequate Testing of the Root Cause of the Error

15. Pro V&V was unable to reliably reproduce the error with the current version of the software, ICX 5.5.10.30. In fact, they reported producing the error only once out of 810 total attempts.

16. Pro V&V appears to have taken Dominion's word for the root cause of the error. The Letter Report does not mention any independent investigation to determine the cause.

17. The description of Pro V&V's first test, using a sample election database, begins with a procedure likely suggested by Dominion—toggling between font sizes to trigger the error. When the 10th toggle produced the error, Pro V&V considered the root cause to be confirmed. That is in itself not unreasonable.

18. However, the same test procedure was later performed using an actual election database, from Douglas County where logic and accuracy testing had revealed the error previously, and 400 toggles and several reboots could not produce the error. Of two test cases that should have both failed, one failed and one did not.

19. Despite these conflicting test results, Pro V&V did not investigate further. They did not consider what might be different between these two test cases to cause contradictory results. They did not consider if the sample election database at the center of their tests was a poor substitute for a real database. They did not consider that the root cause could be different, or that toggling the font size might not be a good trigger for the error.

20. Pro V&V wrote the Letter Report without having confirmed that Dominion's opinion of the root cause was correct.

Inadequate Testing of the Proposed Fix for the Error

21. It is impossible to verify that a proposed change sufficiently addresses an error if the root cause is unconfirmed. A change may only appear to fix the error due to coincidence. Correlation is not causation. A change may incompletely fix the error or create subtle side effects.

22. I have learned this lesson many times while fixing software bugs during my 23 years as a programmer, and I teach that lesson in a course on

software testing. I have also had the practical experience of taking a car to the auto mechanic over and over as they try different solutions for an uncertain cause.

23. Pro V&V's basis for determining that the error was fully resolved by the proposed change, ICX 5.5.10.32, was that the error was not observed after 400 toggles and several reboots.

24. This is not an ideal test case because "absence of evidence is not evidence of absence." The conclusion requires an assumption that subsequent attempts would not surface the error. Given that the first test required only 10 toggles to trigger the error, after 400 toggles and several reboots I might have made a similar assumption.

25. However, when Pro V&V performed the subsequent test on the Douglas County database and also could not observe the anticipated error after 400 toggles and several reboots, they did not revisit their conclusion about ICX 5.5.10.32. They should have.

26. They did not consider that the error could be eluding them in ICX 5.5.10.32 as it was with ICX 5.5.10.30 using Douglas County's database. They did not consider that their assumption that 400 toggles was enough to surface the error was wrong. They did not consider that the proposed change might be an insufficient remedy for the problem.

27. To be clear, I am not suggesting that Dominion's opinion of the root cause is incorrect or that Dominion's proposed change does not fix it. I am saying that testing was insufficient to verify either one. Pro V&V showed no skepticism about their findings when the results created a logical fallacy.

28. Even more surprising, Pro V&V had a real election database from Douglas County in hand, yet they did not test it with ICX 5.5.10.32. The stated purpose of this eleventh-hour software change was to resolve this error for the current election database, rather than create and distribute a new one. The test lab hired to confirm that the new software will work with the current database in a matter of days did not even check.

29. Pro V&V wrote the Letter Report without having confirmed that Dominion's proposed fixed correctly addressed the error, neither on the sample election database nor on the election county database counties are planning to use.

Inadequate Testing of "De Minimis"

30. The EAC defines a de minimis change as:

> A de minimis change is a change to a certified voting system's hardware, software, TDP, or data, the nature of which will not materially alter the system's reliability, functionality, capability, or

operation. Under no circumstances shall a change be considered de minimis if it has reasonable and identifiable potential to impact the system's performance and compliance with the applicable voting Standard.[1]

31. The Letter Report does not describe any testing to demonstrate that the nature of the proposed change does not "materially alter the system's reliability, functionality, capability, or operation" and does not have a "reasonable and identifiable potential to impact the system's performance and compliance with the applicable voting Standard."

32. Pro V&V ignored these critical, foundational requirements in their testing.

33. Pro V&V did not test whether *any* other functionalities of the device are impacted. They did not test whether the new build of the software correctly selects candidates in a series of contests and accurately prints them on a ballot. They did not test other screens to ensure that a fix to the two-column layout did not break another. They did not check if it was still possible to change languages or screen contrast, or whether the audio ballot, used by voters with disabilities, was still working. They did not test whether the device's security was impacted.

---

[1] "Testing and Certification Program Manual," Section 3.4.2, available at: https://www.eac.gov/sites/default/files/eac_assets/1/6/Cert_Manual_7_8_15_FINAL.pdf

34. Pro V&V did not answer the litmus test for de minimis. Does the change materially alter the system's reliability, functionality, capability, or operation?

35. The Letter Report describes "functional regression testing," which might help answer this question, but it misuses the term.

36. Regression testing is a "re-running functional and non-functional tests to ensure that previously developed and tested software still performs after a change."[2] It is so named because a regression is a step backwards in the development of software, the proverbial "two steps forward, one step back."

37. Pro V&V examined the rendering of the two-column layout in their tests. Regression testing would validate that *other* parts of the software still perform correctly.

38. Regardless of Pro V&V's determination, this change is not a de minimis change until the EAC reviews it and approves in writing. "The EAC has sole authority to determine whether any VSTL endorsed change constitutes a de minimis change under this section. The EAC will inform the Manufacturer and VSTL of its determination in writing."[3]

---

[2] "Regression Testing", Wikipedia, available at https://en.wikipedia.org/wiki/Regression_testing

[3] "Testing and Certification Program Manual," Section 3.4.3

39. The EAC prohibited *any* software changes to be considered de minimis until recently out of concern that even small changes might alter the system functionality, due to potential ripple effects I described earlier.

40. Given that the process is new, I expect that the EAC will scrutinize any request for a software de minimis change carefully. I expect the EAC to ask for more rigorous testing and reporting than the Letter Report.

Concerns about the Time Remaining for Review and Testing

41. In my previous declaration I expressed concern about a software change at this late date and fear that time pressures may result in less thorough review and testing of the proposed change.

42. The Letter Report is a wholly inadequate review. Its tests are incomplete.

43. The EAC has not yet begun to review this proposed software change. Using the revised software without the EAC's approval will void the federal certification. EAC approval must be granted in the next five business days to allow early voting to commence on the following Monday.

44. Yet the uncertified software has been distributed and counties have been instructed to install it on over 30,000 ImageCast X devices and to begin testing them.

45. Last week, I heard Michael Barnes describe the current procedures for logic and accuracy testing. The procedures do not test every device, for every ballot style, for every candidate. The procedures do not include any additional testing related to this error. This problem and others could pass through logic and accuracy testing undetected.

Executed on this date, October 4, 2020.

Kevin Skoglund

EXHIBIT E

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

Qualifications and Background

1. I am Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley, where I am also a faculty member in the Graduate Program in Computational Data Science and Engineering; a co-investigator at the Berkeley Institute for Data Science; principal investigator of the Consortium for Data Analytics in Risk; director of Berkeley Open Source Food; and affiliated faculty of the Simons Institute for the Theory of Computing, the Theoretical Astrophysics Center, and the Berkeley Food Institute. Previously, I was Chair of the Department of Statistics and Director of the Statistical Computing Facility.
2. I have published more than one hundred and ninety articles and books. I have served on the editorial boards of archival journals in physical science, Applied Mathematics, Computer

Science, and Statistics. I currently serve on four editorial boards. I have lectured at universities, professional societies, and government agencies in thirty countries. I was a Presidential Young Investigator and a Miller Research Professor. I received the U.C. Berkeley Chancellor's Award for Research in the Public Interest, the Leamer-Rosenthal Prize for Open Social Science, and a Velux/Villum Foundation Professorship. I am a member of the Institute for Mathematical Statistics and the Bernoulli Society. I am a Fellow of the American Statistical Association, the Institute of Physics, and the Royal Astronomical Society. I am professionally accredited as a statistician by the American Statistical Association and as a physicist by the Institute of Physics.

3. I have consulted for many government agencies, including the U.S. Department of Justice, the U.S. Department of Agriculture, the U.S. Department of Commerce, the U.S. Department of Housing and Urban Development, the U.S. Department of Veterans Affairs, the Federal Trade Commission, the California Secretary of State, the California Attorney General, the California Highway Patrol, the Colorado Secretary of State, the Georgia Department of Law, and the Illinois State Attorney. I currently serve on the Board of Advisors of the U.S. Election Assistance Commission and on the Board of Directors of Verified Voting Foundation. (The opinions expressed herein are, however, my own: I am not writing as a representative of any entity.)

4. I have testified before the U.S. House of Representatives Subcommittee on the Census; the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments; the State of California Assembly Committee on Elections and Redistricting; the State of California Senate Committee on Natural Resources; and the State of California Little Hoover Commission.

5. I have been an expert witness or non-testifying expert in a variety of state and federal cases, for plaintiffs and for defendants, in criminal matters and a range of civil matters, including, *inter alia*: truth in advertising, antitrust, construction defects, consumer class actions, credit risk, disaster relief, elections, employment discrimination, environmental protection, equal protection, fairness in lending, federal legislation, First Amendment, import restrictions, insurance, intellectual property, jury selection, mortgage-backed securities, natural resources, product liability class actions, *qui tam*, risk assessment, toxic tort class actions, trade secrets, utilities, and wage and hour class actions. Much of that work concerned statistical sampling and extrapolation.
6. I have been qualified as an expert on statistics in federal courts, including the Central District of California, the District of Maryland, the Southern District of New York, and the Eastern District of Pennsylvania.
7. I have also been qualified as an expert on statistics in state courts.
8. I have used statistics to address a wide range of questions in many fields.[1]
9. I served on former California Secretary of State Debra Bowen's Post-Election Audit Standards Working Group in 2007.
10. In 2007, I invented a statistical approach to auditing elections ("risk-limiting audits") that has been incorporated into statutes in California (AB 2023, SB 360, AB 44, AB 2125), Colorado (C.R.S. 1-7-515), and Rhode Island (RI Gen L §17-19-37.4 (2017)), and which were recently

[1] For example, I have used statistics to analyze the Big Bang, the interior structure of the Earth and Sun, the risk of large earthquakes, the reliability of clinical trials, the accuracy of election results, the accuracy of the U.S. Census, the risk of consumer credit default, the causes of geriatric hearing loss, the effectiveness of water treatment, the fragility of ecological food webs, risks to protected species, the effectiveness of Internet content filters, high-energy particle physics data, and the reliability of models of climate, among other things.

proposed in federal legislation (the PAVE Act of 2018). RLAs have been tested in California, Colorado, Indiana, Ohio, Virginia, and Denmark.

11. RLAs are widely viewed as the best way to check the accuracy of vote tabulation. They have been endorsed by the Presidential Commission on Election Administration, the National Academy of Sciences report "Securing the Vote: Protecting American Democracy," the American Statistical Association, the League of Women Voters, Verified Voting Foundation, Citizens for Election Integrity Minnesota, and other groups concerned with election integrity.
12. I have worked closely with state and local election officials in California and Colorado to pilot and deploy RLAs. The software Colorado uses to conduct RLAs is based on software I wrote.
13. I worked with Travis County, Texas, on the design of STAR-Vote, an auditable and end-to-end cryptographically verifiable voting system.
14. I testified as an expert witness in the general area of election integrity, including the reliability of voting equipment, in 2016 presidential candidate Jill Stein's recount suit in Wisconsin, and filed a report in her suit in Michigan.
15. I have testified as an expert in election auditing and the accuracy of election results in two election-related lawsuits in California.
16. I have testified to both houses of the California legislature regarding election integrity and election audits. I have testified to the California Little Hoover Commission about election integrity, voting equipment, and election audits.
17. Since 1988, I have taught statistics at the University of California, Berkeley, one of the top two statistics departments in the world (see, e.g., QS World University Rankings, 2014) and the nation (US News and World Reports, 2014). I teach statistics regularly at the

undergraduate and graduate levels. I have created five new statistics courses at Berkeley. I developed and taught U.C. Berkeley's first online course in any subject, and among the first approved for credit throughout the ten campuses of the University of California system. I also developed and co-taught online statistics courses to over 52,000 students, using an online textbook and other pedagogical materials I wrote and programmed.

18. Appendix 1 is my current *curriculum vitae*, which includes my publications for the last ten years and all cases in the last four years in which I gave deposition or trial testimony.

Opinions

19. I am offering my opinion with respect to the need and feasibility for Georgia to conduct the 2018 mid-term election using paper ballots and to verify the outcomes of the election using a risk-limiting audit conducted affordably using current voting equipment.

20. The September 6, 2018 National Academy of Sciences, Engineering and Medicine report, *Securing the Vote: Protecting American Democracy*[2] ("the NAS report"), echoes the opinions of leading voting system scientists and the election integrity community: to ensure that reported election results reflect the will of voters, public elections should be conducted with hand-marked paper ballots or systems with a voter-verifiable paper trail.

21. The NAS report recommended that "every effort should be made to use human-readable paper ballots in the 2018 federal election." NAS Report, at 7.

[2] https://www.nap.edu/read/25120/chapter/1 Last accessed 9 September 2018.

22. The Board of Advisors of the U.S. Election Assistance Commission (EAC) passed a resolution in 2018 recommending that the EAC "not certify any system that does not use voter-verifiable paper as the official record of voter intent."[3]

23. Merely using paper ballots to conduct an election does not ensure that results are correct. The paper must actually be used in an appropriate way to check the reported results and to correct the results if they are wrong. Suitable "post-election audits" that manually inspect random samples of paper ballots can detect and correct incorrect electoral outcomes.

24. The NAS report states, "each state should require a comprehensive system of post-election audits of processes and outcomes." NAS Report, at 8. "Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast." NAS Report, at 9.

25. Elections should be conducted in a way that gives the public convincing evidence that reported election outcomes are correct. This is the principle of "evidence-based elections."[4]

26. It is my understanding that since the security breach of the Kennesaw State University Center for Election Systems server, there has been no forensic examination or remediation of voting system components, including many thousands of pieces of computerized election equipment indirectly connected to that server. As a result, in Georgia, the accuracy and trustworthiness of election results are in particular peril compared to most states: the need for paper ballots and rigorous post-election audits is urgent. The paperless systems currently deployed in Georgia simply cannot provide trustworthy evidence that reported election outcomes are correct.

---

[3] https://www.eac.gov/documents/2018/04/27/resolution-2018-03-auditability-of-voter-intent-passed-10-8-4-advisors-resolution-page/ Last accessed 9 September 2018.

[4] Stark, P.B., and D.A. Wagner, 2012. Evidence-Based Elections. *IEEE Security and Privacy, 10*, 33–41. Preprint: https://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf

27. A "risk-limiting audit" (RLA)[5] is a particular approach to catching and correcting incorrect election outcomes before they become official. A RLA is any post-election procedure that offers the following statistical guarantee: If a full manual tally of the complete voter-verifiable paper trail would show a different electoral outcome, there is a known, pre-determined minimum chance that the procedure will lead to a full manual tally.

28. If the procedure does lead to a full manual tally, the result of that manual tally replaces the reported outcome, thereby correcting it.

29. Here, "outcome" means the political result: the candidate(s) or position that won, or the determination that a run-off is needed, not the exact vote totals.

30. The maximum chance that the procedure will not lead to a full manual tally if that tally would show a different outcome is called the *risk limit*. Equivalently, the risk limit is the largest chance that the audit will fail to correct an outcome that is incorrect, where "incorrect" means that a full manual tally of the voter-verifiable paper trail would find different winner(s).

31. For instance, a RLA with a risk limit of 5% has at least a 95% chance of requiring a full manual tally, if that tally would show an outcome that differs from the reported outcome.

32. The NAS Report recommends RLAs: "States should mandate risk-limiting audits prior to the certification of election results." NAS Report, at 9. "Risk-limiting audits can efficiently establish high confidence in the correctness of election outcomes—even if the equipment

[5] Risk-limiting audits have been endorsed by the Presidential Commission on Election Administration, the American Statistical Association, the League of Women Voters, Common Cause, Verified Voting Foundation, and many other organizations concerned with election integrity. They are required by law in Colorado and Rhode Island, and have been tested in California, Ohio, and Denmark. They were developed in 2007; the first publication is Stark, P.B., 2008. Conservative Statistical Post-Election Audits, *Ann. Appl. Statistics*, 2, 550–581. Reprint. Since then, there have been extensions for other social choice functions (e.g., proportional representation, see Stark, P.B., and V. Teague, 2014. Verifiable European Elections: Risk-limiting Audits for D'Hondt and Its Relatives, *JETS: USENIX Journal of Election Technology and Systems*, *3*, 18–39. https://www.usenix.org/system/files/jets/issues/0301/overview/jets_0301_stark_update_9-10-15.pdf), for auditing any number of contests simultaneously, for different types of voting equipment, etc. For a general but still somewhat technical introduction, see Stark, P.B., and M. Lindeman, A Gentle Introduction to Risk-Limiting Audits, *IEEE Security and Privacy*, *10*, 42–49, doi:10.1109/MSP.2012.56

used to cast, collect, and tabulate ballots to produce the initial reported outcome is faulty." NAS Report, at 100.

33. The US Election Assistance Commission (EAC) recently issued a white paper on the history, importance, and conduct of RLAs.[6]

34. It is crucial to base post-election audits on voter-verifiable paper records; to ensure that those records include every validly cast vote exactly once, and no others (checking the determination of eligibility, in particular); to ensure that those records remain complete and intact from the moment they are cast through the audit; and to assess the evidence that they are trustworthy. Absent affirmative evidence that the paper trail is a trustworthy record of voter intent—that it accurately reflects the intent of every voter who legitimately cast a ballot in the contests under audit, and no others—the audit might simply confirm the incorrect outcome. The process of assessing the trustworthiness of the paper trail is called a *compliance audit*.

35. There are many methods for conducting risk-limiting audits, involving different ways of drawing samples of ballots and different demands on the voting system and on auditors. For instance, a full handcount is a risk-limiting audit, with a risk limit of zero. But by inspecting randomly selected ballots and using appropriate statistical methods, it is possible to conduct risk-limiting audits much more efficiently—when the electoral outcome is correct. Below, I discuss *ballot-polling* RLAs, a particular approach that Georgia could implement in time for the 2018 mid-term elections.

36. RLAs require manually inspecting voter-verifiable paper ballots. In particular, digital images of ballots are not a trustworthy record of voter intent.

---

[6] https://www.eac.gov/assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf Last accessed 9 September 2018.

37. Ballot-polling is a particularly simple method for conducting RLAs. It involves selecting and manually inspecting randomly selected cast ballots. If a sufficiently large random sample of ballots shows a sufficiently large margin for the reported winner, that is strong statistical evidence that the reported winner really won.

38. A ballot-polling RLA is similar to an exit poll, but instead of asking a random sample of voters what their preferences were, the audit looks at a random sample individual ballots to see what preferences those ballots show.

39. In contrast to exit polls, the sample size for a ballot-polling RLA is not fixed in advance. A ballot-polling RLA stops if and when the sample shows that it is implausible that anyone other than the reported winner really won. The calculations to determine whether and when the audit can stop are simple enough to be done with a pencil and paper. They involve nothing more complicated than multiplication.

40. The first ballot-polling RLA was conducted in Monterey County, California, in 2011.[7] Since then, they have been used in pilot RLAs in California, Colorado, and Virginia. The first academic papers on ballot-polling RLAs were published in 2012.[8]

41. A free, open-source tool that implements all the calculations for ballot-polling RLAs, including the random selection of ballots and the calculation of when the audit can stop, is available at the URL https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm (last accessed 9 September 2018). That tool is the basis of the software Colorado uses for RLAs in some counties. It has been used in pilot audits in several California and Colorado counties.

---

[7] See http://www.montereycountyelections.us/AB2023.html, last accessed 9 September 2018.

[8] Lindeman, M., P.B. Stark, and V.S. Yates, 2012. BRAVO: Ballot-polling Risk-Limiting Audits to Verify Outcomes. *2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '12)*. Reprint: https://www.usenix.org/system/files/conference/evtwote12/evtwote12-final27.pdf. Lindeman, M. and P.B. Stark, 2012. A Gentle Introduction to Risk-Limiting Audits. *IEEE Security and Privacy*, *10*, 42–49. Preprint: https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

42. Georgia could use ballot-polling RLAs to confirm electoral outcomes if it conducted elections using paper ballots counted by Accu-Vote optical scanners.

43. There are other approaches to RLAs that generally involve inspecting fewer ballots, but that require more data from voting systems and have higher set-up costs than ballot-polling RLAs. For instance, *ballot-level comparison* RLAs are currently the most efficient approach, as measured by the number of ballots that must be audited when the electoral outcome is correct. Georgia should explore other approaches to RLAs in the future, but the easiest RLA method to implement by the mid-term elections is ballot polling.

44. I understand that audit guidelines might need to be established by the Georgia State Election Board in a public process. Because there is now considerable experience conducting RLAs, a great deal of public information, free software, and model legislation, the work could be done in time to audit the 2018 mid-term elections. The fact that Georgia uses a uniform voting system employing the Accu-Vote optical scanner will simplify the process. However, there is no time to waste: work should start immediately.

45. The audit guidelines should embody a number of principles, including requiring serious checks of the integrity of the paper trail, specifying risk limits, specifying how contests subject to RLAs are to be selected, ensuring that the audit cannot be subverted, and providing the public enough information to verify that the audit did not stop prematurely. The guidelines also need to specify how to interpret voter intent from hand-marked ballots.[9]

[9] For instance, if a voter makes a write-in vote for a candidate who is also listed on the ballot, is that a valid vote? If a voter marks a vote for a listed candidate and also writes in that candidate's name, is that a valid vote? If a voter marks a vote for a candidate, crosses through the mark, and marks a vote for a second candidate, is that a valid vote for the second candidate? If a voter makes a stray mark on the ballot that is distinctive enough to identify the ballot, is the ballot valid? Experience in recounts in Minnesota suggests that the percentage of hand-marked ballots that are marked ambiguously is quite small: in the 2008 Minnesota statewide recount, only 845 ballots were challenged. http://minnesota.publicradio.org/collections/special/2008/campaign/results/mn/recount/ballots/ Last visited 9 September 2018. See http://minnesota.publicradio.org/features/2008/11/19_challenged_ballots/ (last visited 9 September 2018) for specific examples.

46. The largest hurdle is to establish procedures that ensure that the paper ballots are physically secured and organized well enough to draw a random sample.

47. In particular, a key ingredient of ballot-polling RLAs is a *ballot manifest* that describes, for each jurisdiction, how many ballots were cast in that jurisdiction and how the ballots are organized.

48. For instance, a ballot manifest might say, "the county has 913 boxes of ballots, numbered 1 through 913. Box 1 contains 301 ballots. Box 2 contains 199 ballots. . . . and Box 913 contains 247 ballots."

49. Ballot manifests should be constructed without reliance on the system that is used to tabulate the votes, because they are used to check the tabulation system.

50. It is reasonable to require local election officials to construct ballot manifests routinely: if an election official cannot keep track of ballots, the official is not doing his or her job.

51. All contests should receive some scrutiny. However, it may be impractical to audit every contest to a pre-specified risk limit. If the guidelines do not require every contest to be audited to a pre-specified risk limit, the selection of contests to audit to a risk limit should involve a random element so that every contest has some chance of being selected and a malicious opponent cannot predict whether any particular contest will be audited.

52. For every ballot selected for audit, votes on that ballot in contests that are not required to be audited to a risk limit should nonetheless be recorded (and reported) to provide evidence about whether the results of those contests are accurate. Collecting such data opportunistically from ballots that are manually inspected enables "risk-measuring audits," which report the strength of evidence that the outcomes of those contests are correct, in light of what the audit finds.

53. The audit sample must not be predictable before the audit starts. Public trust in audits may be increased if the public participates in generating "seed" for selecting the sample. In Colorado, for instance, the "seed" is generated in a broadcast, public ceremony in which 10-sided dice are rolled 20 times, with public participation.

54. Auditing cross-jurisdictional contests requires contest-level results (not merely county-level results) to be known before the audit can conclude. It also requires coordinating the sampling in different counties, so that each county knows when its portion of the audit can stop.

55. I recommend that starting with the 2018 mid-term election, Georgia conduct ballot-polling RLAs of all countywide, statewide, and federal contests, using a risk limit no larger than 5 percent. I recommend that other contests be audited "opportunistically" as described in paragraph 52, *supra*. I believe this is feasible and affordable, but there is no time to waste: the process for establishing the guidelines and procedures must start immediately.

56. A number of non-partisan, non-profit organizations are ready and able to assist Georgia in implementing post-election audits, including Verified Voting Foundation. The U.S. Election Assistance Commission also has staff with extensive experience with RLAs.

57. Although ballot-polling RLAs are not particularly costly, I understand that federal HAVA funds recently granted to Georgia could be used to implement post-election audits, presumably including the cost of monitoring the audits and reporting the results to this Court.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, 9 September 2018.

Philip B. Stark

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my statement of September 9, 2018 regarding the need for post-election audits generally, and in Georgia specifically. I stand by everything in the previous declaration, but in light of the court's decision to allow the State of Georgia to conduct the November 2018 elections using its current equipment, I wish to add a few recommendations.
2. I understand that in the upcoming 6 November 2018 election, some voters will cast their votes using polling-place DRE machines. I understand that other voters will cast paper ballots that will be tabulated using Diebold Accu-Vote optical scanners.
3. There is no way to ensure that DREs correctly record and tabulate votes, because there is no voter-reviewed, durable, tamper-evident record of the votes cast on DREs, and it is possible to alter DRE software undetectably. Unless so few voters cast their votes using DREs that those votes cannot change the outcome of the contests under audit, there is no

way to audit election outcomes in Georgia that guarantees a high probability of detecting and correcting incorrect election outcomes (i.e., a *risk-limiting audit*).

4. Nonetheless, I recommend that a sample of DREs be audited forensically, both before the election (but after the DREs have been configured for the election) and after the election. I recognize that there might not be time for a complete forensic examination of machines before contest results are certified, owing to the short canvass period in Georgia. However, such an examination should be conducted as soon as possible after the election, to inform the conduct of future elections.
5. The forensic examination should be performed by appropriate independent security experts and/or suitably skilled law enforcement personnel. While such examination cannot be guaranteed to detect all tampering, bugs, or hacking, it could detect some kinds of problems and it could discourage malicious tampering.
6. The sample of machines inspected forensically after the election should include any machines for which the reported results are suspicious or anomalous, for instance, because they report more votes than the number of voters reflected in the pollbooks, or because they report a surprisingly large number of undervotes in one or more contests.
7. The samples should also include a number of randomly selected machines. The number of machines selected randomly for forensic auditing after the election should be large enough to ensure that if a material number of DREs used in the election had their software or firmware altered detectably, there is a large chance that the forensic audit will find at least one such machine. The number of machines that should be considered material depends in part on contest margins and the number of votes cast on each DRE. If the court orders the state to conduct such audits, I will gladly make myself available to

determine appropriate sample sizes, to draw the random sample, and to conduct other statistical calculations as needed.

8. I recommend that there be manual checks of the accuracy with which DRE results are reflected in the reported, aggregated contest results: every uploaded electronic tally from a DRE should be checked manually against the totals printed in the polling place when the polls close on election night. The DRE results should also be checked for obvious problems, such as reporting more votes than voters at a polling place.

9. I also recommend that the accuracy of the tabulation of the votes on paper ballots be checked by a post-election audit involving manually inspecting a random sample of ballots, as described below. Even though perfect tabulation of the votes cast on paper ballots cannot in general guarantee that contest outcomes are correct (because some votes are cast on DREs), auditing the accuracy of the tabulation of votes cast on paper ballots is valuable for many reasons, including as a deterrent.

10. I recommend auditing the tabulation of as many contests as practicable, giving priority to statewide and federal contests. The method of determining which contests to audit is not crucial, provided it is not possible for anyone to know which contests will not be audited before election results have been announced. Otherwise, a malicious actor could avoid any possibility of detection. An example of a reasonable rule would be to audit every statewide and federal contest, and a random sample of three within-county contests in each county.

11. I recommend recording voter intent for every contest represented on every ballot inspected by the audit, even contests that are not the deliberate target of the audit, and

making those data publicly available. Such data can provide additional information about the accuracy of the tabulation of other contests at negligible marginal cost.

12. For contests deliberately subject to audit, I suggest that the audit ensure with at least 95 percent confidence that the error (in votes) in the tabulation does not exceed the margin of the contest (in votes), times the percentage of ballots in the contest that were cast using paper ballots. In California law, this is called a "partial risk-limiting audit."
13. Statistical methods and example software that could be used to perform such audits are given in Ottoboni, K., P.B. Stark, M. Lindeman, and N. McBurnett, 2018 (in press). Stratified Union-Intersection Tests of Elections (SUITE), *Electronic Voting. E-Vote-ID 2018*. Lecture Notes in Computer Science, Springer. Preprint: https://arxiv.org/abs/1809.04235, last visited 29 September 2018. If the court orders such post-election audits, I will gladly make myself available to help design and conduct the audit, including providing software to support the audits, and training for election officials.
14. If Georgia election officials undertake post-election auditing of paper ballots, I urge that they consult with non-profit organizations experienced in post-election risk-limiting audits to tailor existing procedures to Georgia's circumstances quickly, inexpensively, and reliably. The procedures need to ensure that the paper records remain trustworthy, through measures such as ballot accounting, verified chain of custody, two-person access rules, and appropriate physical security and surveillance.
15. Post-election auditing has no impact on voters' experience casting their votes nor on pollworkers' duties at the polling places: the audit is conducted in the election officials' offices after polls close, not at polling places.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, September _30,_ 2018.

Philip B. Stark

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRAD RAFFENSPERGER, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

SECOND SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my statements of September 9, 2018, and September 30, 2018. I stand by everything in the previous declarations.
2. I understand that the State of Georgia proposes to deploy ballot-marking devices (BMDs) for all in-person voters. In my opinion, this will do little to improve election integrity in Georgia: BMDs are essentially as vulnerable as the DRE machines they would replace, despite the fact that BMDs generate a "voter-verifiable" paper trail. I shall explain why.
3. I understand that Defendants argue that a BMD-based system is auditable, and that therefore BMD-based voting systems are acceptable. The premise is misleading and the conclusion is false.
4. Every system is auditable—to some extent. The question is not whether a BMD-based system can be audited in some sense. The question is what audits of BMDs can

accomplish, and in particular, whether they can reliably detect whether software bugs, errors, or hacking altered the reported election results. Audits of BMDs cannot.

5. This is in part because BMDs make the paper audit trail vulnerable to malfunctions. Bugs, misconfiguration, or malicious hacking can cause the BMD to print something other than the selections the voter made on the touchscreen or accessible interface. Hand-marked paper ballots do not have that vulnerability.

6. Audits of BMDs cannot reliably detect whether malfunctioning BMDs corrupted the paper trail. (I use the term *malfunction* generically to include problems due to bugs, configuration errors, and hacking.) This is true even if the malfunctions were severe enough to cause losing candidates to appear to win.

7. If an audit or inspection of a BMD happens to discover a malfunction, there is in general no way to tell whether the malfunction altered electoral outcomes, nor any way to determine the correct electoral outcomes.

8. Because a BMD-generated paper trail is not trustworthy, voting systems based largely on BMDs are not *strongly software independent.*[1]

---

[1] See Rivest, R.L., and J. Wack, 2006. On the notion of "software-independence" in voting systems. https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf (last visited 20 October 2019). A voting system is *strongly software independent* "if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome, and moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected without re-running the election." Strong software independence is extremely desirable. Systems based on optically scanning hand-marked paper ballots (with reliable chain of custody of the ballots) are strongly software independent, because inspecting the hand-marked ballots allows an auditor to determine whether malfunctions altered the outcome, and a full manual tabulation from the paper ballots can determine who really won, without having to re-run the election. A risk-limiting audit of an election conducted using hand-marked paper ballots can guarantee a large chance of correcting the outcome if the outcome is wrong. In contrast, because BMD printout cannot be trusted to reflect voters' selections, auditors can only determine whether the BMD printout was tabulated accurately, not

9. Because a BMD-generated paper trail is not trustworthy, voting systems based largely on BMDs cannot support *evidence-based elections*.[2]

10. Only voters are in a position to catch some kinds of BMD malfunction. There is no other mechanism. No feasible amount of parallel or "live" testing or auditing can offer a reasonable chance of catching outcome-changing errors.[3]

11. Even if the vast majority of voters caught and corrected errors in their printout, outcomes as reflected in the BMD paper trail could be wrong, because some contests are decided by small margins.[4]

12. Even if voters notify pollworkers of problems, the way elections are conducted in Georgia (and the rest of the U.S.), there is no mechanism to translate that into remedial action beyond giving voters who complain another chance to mark a ballot. That is partly because voters who observe a problem get no evidence they can show to anyone else to

---

whether the election outcome is correct, nor can auditors determine the correct outcome. Elections conducted using BMDs are not strongly software independent because, if a BMD malfunction happens to be detected, there is no way to figure out what the correct electoral outcome is without re-running the election.

[2] See Stark, P.B., and D.A. Wagner, 2012. Evidence-Based Elections. *IEEE Security and Privacy, 10*, 33-41. https://doi.ieeecomputersociety.org/10.1109/MSP.2012.62 (last visited 22 October 2019) Evidence-based elections require election officials to produce convincing evidence that the reported winner(s) really won. That is not possible if a noticeable fraction of ballots are marked using BMDs. The draft of version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0) requires systems to be software independent and to support evidence-based elections. Draft Voluntary Voting System Guidelines, version 8, 19 September 2019 https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2019-09-17-DRAFT-requirements.pdf (last retrieved 22 October 2019).

[3] See Stark, P.B., 2019. There is no reliable way to detect hacked ballot-marking devices. ArXiV, https://arxiv.org/pdf/1908.08144.pdf (last visited 20 October 2019).

[4] Stark, *op. cit.,* and Appel, A., R. DeMillo, and P.B. Stark, 2019. Ballot-marking devices (BMDs) cannot assure the will of the people, SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755 (last visited 20 October 2019).

demonstrate that there was a problem. Showing a pollworker or election official the BMD printout does not prove anything: it is the voter's word against the BMD output.[5]

13. Research shows that relatively few voters do check, and that they are not good at it.[6]

14. If pollworkers and election officials take voter complaints of BMD malfunctions seriously, their only recourse is to hold a new election. That would make the whole election system vulnerable to "crying wolf."[7]

15. For the reasons above, the reliance on BMDs in elections should be kept to a minimum, and hand marked paper ballots should be the primary voting technology. With luck, there will soon be voting technology that is more accessible and more meaningfully auditable than BMDs—technology that supports "evidence-based elections,"[8] as recommended by Principle 9, "Auditable," in the most recent draft of Version 2.0 of the U.S. Voluntary Voting System Guidelines.[9] Evidence-based elections are not possible if a noticeable percentage of ballots are marked using BMDs.

16. Unless the State of Georgia adopts rigorous post-election audits, including "compliance audits"[10] and risk-limiting audits (RLAs), using a voting system with a paper trail will not improve the trustworthiness of Georgia's elections at all.

---

[5] Appel et al., *op. cit.*
[6] DeMillo, R., R. Kadel, and M. Marks. 2018. What Voters Are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots, SSRN https://ssrn.com/abstract=3292208 (last visited 20 October 2019).
[7] Stark, *op. cit.,* Appel et al., *op. cit.*
[8] See note 2, *supra*.
[9] See note 2, *supra*.
[10] Stark and Wagner, op. cit.; Stark, P.B., 2018. An Introduction to Risk-Limiting Audits and Evidence-Based Elections, Prepared for the California Little Hoover Commission, https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf (last retrieved 21 October 2019).

17. I drafted most of the language defining and explaining RLAs in Georgia's Act 24 (2019-HB316) §21-2-498 (a)-(d). Contrary to my recommendations, Act 24 does not require routine RLAs, only a pilot, which is not required until late 2021.

18. The audit requirements under HB 316 are seriously deficient. An audit could satisfy HB 316 and yet have no chance of discovering or correcting errors, even outcome-changing errors.

19. For instance, HB 316 does not require audits and recounts to be based on the human-readable marks on the paper trail. But a malfunctioning BMD could print barcodes that do not match the human-readable marks.[11] An audit based on the barcodes cannot possibly detect that.

20. HB 316 does not require audits to take any remedial action if they uncover errors in the electronic tally. Such "toothless" audits do little to ensure election integrity.

21. HB 316 does not require any auditing until November 2020. The presidential primary elections will take place sooner. Absent any auditing, the primaries will be vulnerable to outcome-changing errors and malfunctions that would have a large chance of being caught and corrected by a RLA.

[11] A BMD can also print human-readable marks and barcodes that do not match what the voter saw on the touchscreen or heard through the audio interface.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, October 22, 2019.

Philip B. Stark

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

THIRD SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018, September 30, 2018, and October 22, 2019. I stand by everything in the previous declarations.
2. I have read portions of the State Defendants' Combined Response in Opposition to Curling Plaintiffs' and Coalition Plaintiffs' Motions for Preliminary Injunction, dated November 13, 2019 ("Combined Response"). This declaration responds primarily to assertions made in the Combined Response, including the declaration of Juan E. Gilbert, Ph.D., contained therein ("the Gilbert declaration").

AUDITS

3. The most compelling reason for post-election audits is to provide public evidence that the reported outcomes are correct, so that the electorate and the losers' supporters have reason to trust the results. Audits that cannot provide evidence that outcomes are correct

are little comfort. A transparent, full hand count of a demonstrably trustworthy paper record of votes can provide such evidence. So can a risk-limiting audit of a demonstrably trustworthy paper record of votes. The advantage of risk-limiting audits is that they are often more economical and efficient than a full hand count; the disadvantage is that they can fail to correct a wrong outcome. What makes an audit "risk limiting" is that the chance it fails to correct a wrong outcome is guaranteed not to exceed a pre-specified limit, the "risk limit."

4. Indeed, by definition, a risk-limiting audit must have a known minimum chance of correcting the reported outcome if the reported outcome is incorrect. A risk-limiting audit corrects the reported outcome by conducting a full manual tabulation of the votes in the paper trail: just like a recount, it requires a trustworthy paper trail. If there is no trustworthy paper trail, a true risk-limiting audit is not possible, because an accurate full manual recount would not necessarily reveal who won. Because BMD printout is not trustworthy, applying risk-limiting audit procedures to BMD printout does not yield a true risk-limiting audit.

5. Defendants assert that a post-election audit can demonstrate that BMDs function correctly during elections. As I wrote in my October 22, 2019, supplemental declaration, audits of BMD-marked ballots (printouts) cannot reliably detect whether malfunctioning BMDs printed the wrong votes or omitted votes or printed extra votes. (Here, as before, I use the term *malfunction* generically to include problems due to bugs, configuration errors, and hacking.) As I wrote then, that is true even if the malfunctions were severe enough to make losing candidates appear to win.

6. Applying risk-limiting audit (RLA) procedures to securely curated BMD printouts can check the accuracy of the tabulation of the printouts. It can provide confidence that if errors in scanning and tabulation were large enough to change the reported winner(s), that fact would be detected and corrected.

7. But such an audit does *nothing* to check whether the BMDs printed incorrect votes, omitted votes, or printed extra votes. Risk-limiting audit procedures check the *tabulation of BMD printouts*; they do not check the *functioning of the BMDs*. They cannot confirm the outcome of elections conducted using BMDs.

8. Indeed, there is no known pre-election or post-election procedure that can tell reliably whether BMDs will malfunction or did malfunction during an election. Nor is there any practical procedure that can reliably detect outcome-altering BMD malfunctions during an election.[1]

9. Therefore, there is no way to establish that BMD printout is a trustworthy record of what the BMD displayed to the voter or what the voter expressed to the BMD.

10. While it is crucial to maintain secure custody of the election paper trail—whether the paper trail consists of hand-marked ballots or BMD printouts—even if BMD printouts have been maintained verifiably securely, they are not a trustworthy record of what voters did, what they saw on the BMD screen, or what they heard through the BMD audio interface, because there is vulnerable software between the voter and the printout. In contrast, computer hacking, configuration errors, and bugs cannot cause pens to put the wrong marks on hand-marked paper ballots.

[1] Stark, P.B., 2019. There is no reliable way to detect hacked ballot-marking devices. ArXiV, https://arxiv.org/pdf/1908.08144.pdf (last visited 20 October 2019).

11. Voters can err in hand-marking ballots and in using a BMD. But BMD printouts are also vulnerable to bugs, misconfiguration, and hacking; hand-marked paper ballots are not.
12. The tabulation of both kinds of paper record is subject to bugs, misconfiguration, and hacking. Rigorous audits can ensure (statistically) that tabulation errors did not alter the reported outcomes. But they cannot ensure that errors in BMD printouts did not alter the reported outcomes.
13. Some voters check their BMD printouts, and, if they notice errors, will request a fresh opportunity to vote. But unless virtually every voter diligently checks the printout before casting it, there is no reason to believe that an accurate tabulation of BMD printouts will show who really won.
14. The evidence suggests that less than ten percent of voters check their printouts, and that voters who do check often overlook errors. See paragraph 30(d), *infra*. As a result, errors in universal-use BMD printouts could alter margins by very large amounts: virtually every contest is decided by fewer votes than undetected, uncorrected errors in BMD printouts could produce.
15. But even if ninety percent of voters check their printouts and correct any errors they find, misprinted votes on the remaining ten percent of printouts could alter a reported margin by twenty percent (or even more than twenty percent, for contests that are not on every ballot). Many contests are decided by margins of less than twenty percent.
16. In an actual election, there is no way to know how many voters checked their BMD printouts for accuracy.

THE NOVEMBER 2019 PILOT RISK-LIMITING AUDIT IN GEORGIA

17. I invented risk-limiting audits in 2007 and published the first peer-reviewed papers about them in 2008.[2] I collaborated with election officials in California and Colorado to conduct the first dozen or so pilot RLAs, starting in 2008.[3] In 2011, I invented and published the particular RLA method[4] used in the 2019 pilot audit of two contests in Cartersville, Georgia, conducted with the assistance of Verified Voting and VotingWorks.[5] (I was not involved in the Cartersville pilot audit.) The method, "ballot polling," was published more formally in 2012 in two peer-reviewed papers I co-authored.[6] I provided open-source software implementing ballot-polling RLAs,[7] which became the basis of the State of Colorado RLA regulations, the software the State of Colorado currently uses for its audits, and the Arlo software used for the Georgia pilot audit. Indeed, I understand that VotingWorks, the company that built the Arlo audit

---

[2] Stark, P.B., 2008. Conservative statistical post-election audits, *The Annals of Applied Statistics, 2*, 550–581. Reprint: http://arxiv.org/abs/0807.4005
Stark, P.B., 2008. A Sharper Discrepancy Measure for Post-Election Audits, *The Annals of Applied Statistics, 2*, 2008, 982–985. Reprint: http://arxiv.org/abs/0811.1697

[3] Hall, J.L., L.W. Miratrix, P.B. Stark, M. Briones, E. Ginnold, F. Oakley, M. Peaden, G. Pellerin, T. Stanionis and T. Webber, 2009. Implementing Risk-Limiting Audits in California, *2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '09)*

[4] https://www.verifiedvoting.org/philip-stark-report-on-second-risk-limiting-audit-under-ab-2023-in-monterey-county-california/ (last visited 9 December 2019).

[5] Mark Lindeman, Verified Voting, personal communication, 9 December 2019.

[6] Lindeman, M., P.B. Stark, and V.S. Yates, 2012. BRAVO: Ballot-polling Risk-Limiting Audits to Verify Outcomes. *2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '12*)
Lindeman, M., and P.B. Stark, 2012. A Gentle Introduction to Risk-Limiting Audits. *IEEE Security and Privacy, 10*, 42–49.

[7] https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm (last visited 12 December 2019).

software, used my software as a touchstone to ensure that they had implemented the method correctly.[8]

18. Ballot-polling audits are a bit like exit polls, but instead of asking randomly selected voters how they voted, they manually inspect randomly selected cast ballots to see the votes they contain. If a large enough random sample of ballots shows a large enough majority for the reported winner(s), that is strong statistical evidence that the reported winner(s) really won. It would be very unlikely to get a large majority for the reported winner(s) in a large random sample of ballots if the true outcome were a tie, or if some other candidate(s) had won. There is deep mathematics behind proving out how large is "large enough" to control the risk to a pre-specified level, such as five percent. However, the calculations that determine when the audit can stop examining more ballots are relatively simple.

19. No auditing method can check whether BMD printout correctly recorded voters' expressed intent.

20. Ballot polling, the audit method used in Cartersville, does not check whether any BMD printout was tabulated correctly. Ballot-polling audits only check whether a full hand count of the BMD printout would find the same winners. In particular, the vote tabulation system in Cartersville could have mistabulated every single BMD printout and still passed the audit.

21. The Cartersville pilot audit did not—and in principle could not—confirm that the reported outcomes were correct, because it did not and could not show that the BMDs functioned correctly. All the audit did was provide statistical evidence that a full manual

[8] Ben Adida, VotingWorks, personal communication, 8 November 2019.

tabulation of the BMD printouts would find the same winners that were reported in the two audited contests. If the BMD printouts contained outcome-changing errors, the audit would have had no chance of detecting that, nor of correcting the reported outcomes.

22. In contrast, if the election had been conducted with hand-marked paper ballots and those ballots had been properly secured, the same audit procedure could have provided strong evidence that the reported winners really won.

23. I resigned from the Board of Directors of Verified Voting Foundation over their president's refusal to clarify publicly that the Cartersville pilot audit did not "confirm outcomes" or show that the voting system worked correctly.

THE NATIONAL ACADEMIES REPORT

24. Defendants claim that the 2018 National Academies of Science, Engineering, and Medicine report *Securing the Vote: Protecting American Democracy* ("NASEM Report") recommends BMDs. In fact, the NASEM Report draws important distinctions between BMDs and hand-marked paper ballots, and points out that additional research on BMDs should be conducted before BMDs are deployed widely:

    a. "The U.S. Election Assistance Commission, National Institute of Standards and Technology, U.S. Department of Homeland Security, National Science Foundation, and U.S. Department of Defense should sponsor research to: [] determine voter practices regarding the verification of ballot marking device–generated ballots and the likelihood that voters, both with and without disabilities, will recognize errors or omissions[.]" NASEM Report, at 11–12.

b. "Research suggests that DRE VVPATs[9] tend not to be voter verified. This suggests that VVPATs may be of little value as a check on the accuracy of DREs. See, e.g., Everett, S. P., "The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection," doctoral dissertation, Rice University, Houston, Texas and Campbell, Bryan A. and Michael D. Byrne, "Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability," Proceedings of EVT/WOTE, 2009. Research on the rate of voter verification of BMD ballots relative to the rate of verification of VVPATs or voter-marked paper ballots has been limited." NASEM Report, at 44.

c. "Unless a voter takes notes while voting, BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent."[10] NASEM report, at 79.

d. "By hand marking a paper ballot, a voter is, in essence, attending to the marks made on his or her ballot. A BMD-produced ballot need not be reviewed at all by the voter. Furthermore, it may be difficult to review a long or complex BMD-produced ballot. This has prompted calls for hand-marked (as opposed to BMD-produced) paper ballots whenever possible." NASEM Report, at 79.

25. Recent congressional testimony of Dr. Matt Blaze of Georgetown University[11] echoes these concerns:

---

[9] VVPAT stands for "voter-verified paper audit trail," a printout similar to a cash register receipt that some DREs provide. As explained by NASEM, such receipts are rarely "verified" by voters: the acronym is a misnomer.

[10] I understand that the BMDs Georgia is using are of this type.

[11] Blaze, Matt. Testimony Before the US House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. Hearing on Defending Against Election Interference, November 19, 2019.

> "BMD-based voting systems are controversial, since, by virtue of their design, the correctness of their behavior cannot be effectively audited except by every individual voter carefully verifying his or her printed ballot before it is cast. A maliciously compromised BMD could subtly mismark candidate selections on ballots in a way that might not be noticed by most voters. If BMDs fail or must be rebooted at a polling place, there may be no way for voters to create marked ballots, making BMDs a potential bottleneck or single point of failure on election day.
>
> As a relatively new technology, BMD-based systems have not yet been widely examined by independent researchers and have been largely absent from practical election security research studies. However, even with relatively little scrutiny, exploitable weaknesses and usability flaws have been found in these systems. This underscores the need for more comprehensive studies and for caution before these systems are purchased by local jurisdictions or widely deployed." Blaze testimony, at 8.

26. Defendants claim that "Plaintiffs cannot point to any real security risk or hacking potential the use of BMDs poses." There are countless studies showing that BMDs and other electronic voting equipment have serious security vulnerabilities and can be hacked. The 2018 Def Con Voting Village Report found easily exploited vulnerabilities in the

https://www.congress.gov/116/meeting/house/110238/witnesses/HHRG-116-HM08-Wstate-BlazeM-20191119.pdf (last visited 12 December 2019).

Dominion ImageCast Precinct BMD,[12] which I understand is of the same make that Georgia has deployed, but possibly not the identical model.

DR. GILBERT'S DECLARATION

27. Dr. Gilbert questions my credentials regarding election security, dismissing me as a statistician. I am on the cybersecurity subcommittee of the Board of Advisors of the U.S. Election Assistance Commission. I have authored or co-authored more than 15 peer-reviewed articles in journals and conference proceedings on cybersecurity, information forensics, and the security of electronic voting technology; my co-authors are an international who's-who of cybersecurity experts and cryptographers. I have been a keynote speaker at numerous international conferences on cybersecurity and elections. I have given two distinguished lectures at the Center for Security, Reliability, and Trust at the University of Luxembourg. I am the co-author of a report on election forensics for the Venice Commission of the Council of Europe. I have testified to the California legislature on election security several times, and to the California Little Hoover Commission. I have advised the California Secretary of State and the Colorado Secretary of State on mitigating electronic threats to elections. I have advised the governments of Denmark, Nigeria, and Mongolia on election security. I have been a Visiting Professor of Theoretical Computer Science at the IT University of Copenhagen, sponsored by a Velux/Villum Foundation fellowship to work on election cybersecurity. I am regularly on the program committee of two international election security conferences. And, as

[12] https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf at 18–19. (last visited 12 December 2019).

mentioned above, I invented risk-limiting audits, widely regarded to be the best tool for verifying election outcomes even in the face of hacking and computer malfunctions (provided there is a trustworthy paper trail of votes).

28. Dr. Gilbert's expertise related to elections is in usability. He does not represent himself to be an expert in computer security, statistics, or auditing. I have read his CV dated 24 November 2019.[13] His research focuses on usability, accessibility, inclusion, and the use of technology in teaching and mentoring, for instance, making self-driving cars more accessible, inclusive university admission policies, using "chatbots" to mentor graduate students, "designing a humorous workplace," cyberbullying, and similar subjects. He has two refereed paper related to electronic voting in 2012 and 2013. Both are usability studies, not security studies. His only publication in a security-related journal was in 2008, with eight co-authors, introducing a BMD system he helped design. That paper describes the system and some measures they took to secure it but does not include a formal security analysis of the system. He published a paper on risk analysis of software design (not implementation) with three co-authors, in what appears to be an Alabama-based industrial trade show in 2012.[14] I was unable to find a copy of that paper. His credentials in cybersecurity are limited and inapposite.

29. Many of Dr. Gilbert's pronouncements on security and auditability of BMD systems are erroneous. I shall not rebut them all, but I shall point out a few particularly serious errors.

[13] https://www.cise.ufl.edu/~juan/cv.pdf (last visited 14 December 2019)
[14] AlaSim: https://10times.com/alasim (last visited 14 December 2019) "The annual AlaSim International Conference & Exposition showcases the vibrant, multi-domain, modeling and simulation (M&S) industry in Alabama."

30. Defendants claim, partly on the basis of Dr. Gilbert's declaration, that "BMDs are far more like hand-marked paper ballots than they are like DREs." Combined response, at 2; Gilbert declaration, at 11ff. That is not true from the perspective of technology, security, auditability, or evidence. The only thing BMDs have in common with hand-marked paper ballots is that both involve paper tabulated by scanners, while DREs tabulate directly from an electronic record. Aside from that, BMDs (and their attendant risks) are exactly like DREs with VVPAT:

    a. Vulnerable electronic technology is between the voter and the vote record: the paper trail itself is hackable. There is no trustworthy record of the voter's expressed vote with either technology. Both BMDs and DREs can be hacked—from afar, undetectably. Pens have no software to hack.

    b. In contrast to Defendants' claim that for BMDs (and, by implication, DREs) "there are no questions of voter intent" (Combined Response, at 2), BMDs *obscure all direct evidence* voter intent. This is an example of "the ostrich principle": because BMDs make the problems impossible to detect, Dr. Gilbert concludes that the problems do not exist. It is impossible to know from BMD printout what the voter expressed to the machine or what the BMD presented to the voter on the screen or audio interface. In contrast, voter intent can generally be inferred manually from voters' marks on hand-marked paper ballots.[15]

    c. There is no way a voter can prove that a BMD or DRE printed his or her vote incorrectly, so the underlying "security loop" for both technologies is broken in

[15] See the discussion of the Minnesota recounts in Appel, A., R. DeMillo, and P.B. Stark, 2019. Ballot-marking devices (BMDs) cannot assure the will of the people, SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755 (last visited 20 October 2019).

the same way. Neither system generates any evidence a voter can take to an authority or third party to demonstrate that there was a problem.

d. All extant research of which I am aware suggests that voters rarely check BMD printout or DRE printout, and that voters are not good at catching errors in the printout when they do check.[16]

e. Neither DREs nor BMDs are auditable in practice. Pre-election logic and accuracy testing cannot assure that the devices will perform properly on election day. No practical amount of parallel or "live" testing on election day can provide reasonable assurance that the devices record votes accurately.[17] No post-election procedure can determine whether the devices correctly recorded votes during the election.

f. A DRE can be converted into a BMD by adding a printer and making changes to the software. And a BMD can be converted into a DRE by means of changes to the software alone. The same is not true for hand-marked paper ballots.

31. Dr. Gilbert opines that various properties of BMDs make them preferable, on balance, to hand-marked paper ballots. Gilbert declaration, at 11. His declaration generally does not address the security aspects of BMDs, which are at the heart of the issue. Many of his opinions are contradicted by the available data and by his own research.

32. Most of the advantages he claims universal-use BMDs have over hand-marked paper ballots fall into four categories:

[16] In addition to the studies cited by Appel et al. (2019), I am aware of another study of whether and how well voters check BMD printout that is currently in peer review.
[17] Stark, P.B., 2019.

a. *They are not actually advantages*. Issues of ballot layout and design are in this category: bad layout can greatly increase voter errors for both BMDs and hand-marked paper ballots. Indeed, his own work points out examples where bad screen layout and bad user interfaces in touchscreen voting equipment evidently caused a high undervote rate.[18] Undervote protection also falls partly in this category: both BMDs and precinct-count optical scan hand-marked paper ballots can offer protection against undervotes and overvotes (depending on system configuration); however, BMDs offer an "attack surface" that would allow malware to insert votes in contests the voter deliberately chose not to vote in. That cannot occur with hand-marked paper ballots.

b. *They ride on a misuse of terminology*. For instance, he conflates "ambiguous mark" with "a mark a scanner cannot read." Similarly, his conclusion that hand-marked paper ballots are not strongly software independent ignores part of the definition of strong software independence. And he conflates auditing the tabulation of votes with auditing electoral outcomes—which requires a trustworthy paper record of the votes.

c. *The claimed advantages occur only if the BMDs function correctly*. Usability and overvote and undervote protection also fall partly in this category. The primary problem with BMDs is that there is no way to ensure that they function correctly. They are vulnerable to bugs, misconfiguration, and malicious hacking. This was brought home in the recent election in Northampton, PA, where BMDs were

[18] Gilbert, J.E., J. Dunbar, A. Ottley and J.M. Smotherman, 2013. Anomaly detection in electronic voting systems, *Information Design Journal*, *20*(3), 194–206, at 195–196.

miscalibrated and misconfigured. The configuration errors—which were not discovered by pre-election logic and accuracy tests—were so severe that *voter instructions* (rather than candidates) *received thousands of votes*![19]

d. *The advantages might occur for some BMD systems but not others*. Usability advantages fall in this category: he makes blanket statements that BMDs are usable by voters with disabilities. Gilbert declaration, at 19. A number of BMDs have failed usability testing in other states.[20] (Moreover, increases in usability in recording selections electronically are largely undermined, because the equipment cannot be relied upon to print those selections accurately.) Gilbert makes blanket statements about the usability of By his own admission, he has not inspected the BMD system Georgia is deploying. Gilbert declaration, at 16, 20.

33. I now give more specific examples of incorrect security assessments he made.

34. Dr. Gilbert overlooks the fact that BMD printouts have every security vulnerability that hand-marked paper ballots do, *plus* cyber risks that cannot feasibly be mitigated. In

[19] "An instructional message regarding cross-filed candidates created an error in the machines' database. As a result, thousands of electronic votes were mistakenly cast for the instructional message instead of the correct candidate." T. Shortell and Christina Tatu, The Morning Call, 12 December 2019. https://www.mcall.com/news/elections/mc-nws-northampton-county-election-voting-machine-problems-reason-20191212-6icnnb2fqjfw5dencuy73n66wm-story.html, last visited 13 December 2019. According to this report, the manufacturer admits that 30% of the machines were misconfigured—and that the misconfiguration was not detected by pre-election logic and accuracy testing.

[20] For instance, the Dominion Democracy 5.5 system, including the ImageCast Precinct and the ICX Prime BMD, failed testing in Texas for reasons of security and accessibility. https://www.sos.state.tx.us/elections/laws/jan2019_dominion.shtml (last visited 14 December 2019). The ES&S ExpressVote and ExpressVote XL BMDs failed usability testing in Pennsylvania with several "show stopper" flaws; moreover, the review found that it was "possible but challenging" to verify the BMD printout: https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/ESS%20EVS%206021/EVS%206021%20Secretary%27s%20Report%20Signed%20-%20Including%20Attachments.pdf (last visited 14 December 2019)

particular, he makes much of risks involving the physical security of hand-marked paper ballots but ignores the fact that BMD printouts face the same physical security risks (and additional cyber risks).

35. Dr. Gilbert ignores the fragility and unreliability of BMDs and the fact that BMDs produce a bottleneck in the voting process.[21] There are many instances where voting machines did not boot up or misbehaved on election day, preventing voting or undermining voter confidence.[22] Providing an inadequate number of BMDs in polling places will also discourage or prevent voting by creating long lines.

36. He treats risks that require a large conspiracy, insider malfeasance, and physical access to ballots as if they were equivalent to cyber risks, where nation states—or individual hackers—can undetectably alter election results without physical access to any part of the voting system. The primary threats to hand-marked paper ballots are of the first kind. BMDs face exactly the same threats of the first kind, but also face threats of the second

---

[21] See paragraph 25, *supra.*

[22] There are many examples of election equipment failures and malfunctions on election day. Here are a few, including some failures of relatively new or brand new equipment: https://www.mcclatchydc.com/news/politics-government/election/midterms/article221196655.html (last visited 16 December 2019) https://www.postandcourier.com/free-times/news/local_and_state_news/richland-county-failed-to-count-hundreds-of-november-election-ballots/article_849a1c98-c21a-5728-afc5-c58aae39e126.html (last visited 16 December 2019) https://www.commoncause.org/media/south-carolina-voting-machine-failure-underscores-need-for-swift-federal-action-for-voting-security/ (last visited 15 December 2019) https://www.pennlive.com/news/2019/11/gop-officials-file-legal-action-in-pa-after-massive-voting-machine-malfunctions-ballots-placed-in-suitcase.html (last visited 15 December 2019) https://www.kansascity.com/news/politics-government/election/article221198575.html (last visited 16 December 2019) https://www.pbs.org/newshour/politics/which-states-were-hit-by-voting-problems-on-election-day (last visited 16 December 2019) https://www.montgomeryadvertiser.com/story/news/2017/12/12/new-voting-machines-cause-senate-election-problem-montgomery-polling-place/944247001/ (last visited 16 December 2019) https://www.upi.com/Top_News/US/2018/10/26/Texas-voters-report-error-with-electronic-voting-machines/9211540569616/?ilink=1 (last visited 16 December 2019)

kind that cannot be controlled by auditing. His discussion of "undervote hacks" and "overvote hacks" on hand-marked paper ballots commits this error.

37. He implies—contrary to the evidence and contradicting his own publications—that voters will catch and correct errors in BMD printout. Every extant study I know of finds that voters rarely check BMD printout, and that when they check, they often fail to notice errors that are present. This is consistent with research on DRE printouts also.[23] His own publications cite research that "no more than half of study participants notice [voting machine] review screen anomalies."[24,25]

38. He claims that BMDs and hand-marked paper ballots are equally auditable. The *tabulation* of both kinds of paper record can be audited, but no practical amount of auditing can offer any assurance that *BMDs themselves* did not malfunction and were not hacked to produce erroneous paper records.[26]

39. The advantages Dr. Gilbert claims BMDs have (undervote and overvote protection, accessibility, etc.) are predicated on the BMDs functioning correctly. But that is precisely the problem: BMDs cannot be relied upon to function correctly, nor is there a reliable way to detect malfunctioning BMDs. Moreover, if BMD malfunctions are detected, there is no way to determine which printouts were affected and what the correct electoral outcome is. The only remedy is to hold a new election.

40. Dr. Gilbert's analysis of overvote and undervote protection assumes that what BMDs print is identical to what the BMD shows voters on the screen or presents voters through

[23] See paragraph 24(b), *supra*, and note 16, *supra.*
[24] Gilbert et al., 2013.
[25] Of course, noticing an anomaly on a review screen and noticing an anomaly on BMD printout are not the same task, and a BMD can print something other what the review screen shows.
[26] Stark, P.B., 2019.

audio. That ignores the possibility of BMD malfunctions and hacking. A BMD can print selections that differ from what the voter was presented on the screen or the audio interface. It can omit contests or votes, add contests and votes, and alter votes. BMDs provide *no* protection against overvotes and undervotes created by BMD malfunctions. Dr. Gilbert assumes away the essential problem: BMD technology is not trustworthy.

41. Dr. Gilbert alleges that there is no effective protection against overvotes or undervotes in hand-marked paper ballot systems. In fact, many, if not all, precinct-count optical scan systems for tabulating hand-marked paper ballots can warn voters of undervotes and overvotes, and can return the ballot to the voter if the voter wishes to re-mark the ballot in response, or allow the voter to override the warning and cast the ballot.

42. BMDs are vulnerable to "presentation attacks," where bugs, misconfiguration, or hacking causes the device not to display a contest the voter has a right to vote in (denying the voter the opportunity to vote in that contest). This can *create* undervotes that the BMD would not help the voter "detect." While contests might be omitted from pre-printed paper ballots, standard pre-election procedures can detect that. In contrast, there is no practical procedure—before, during, or after the election—that can provide a reasonable level of assurance that a BMD presented voters the correct opportunities to vote.

43. Dr. Gilbert's concern about "undervote hacks" identifies an important problem with all paper-based systems, including BMDs: the paper trail must be kept demonstrably secure from additions, subtractions, substitutions, and alterations. That is just as true for BMD printouts as it is for hand-marked paper ballots. A crucial difference he omits, however, is that altering hand-marked paper ballots is intrinsically a "retail" fraud problem: it takes many people, a lot of time, and physical access to the ballots to alter a large number of

ballots. In contrast, BMD printouts are subject to "wholesale" fraud and error as a result of bugs, hacking, or misconfiguration. It does not require many accomplices or physical access to the voting system or the printouts to alter outcomes of elections conducted on BMDs.

44. He expresses concern that systems that lack undervote protection (meaning hand-marked paper ballots) will have disparate impact on minority voters, citing experience in 2000. Gilbert declaration, at 27. More recent data belie this claim. I understand that the DREs in use in Georgia in the 2018 election had undervote protection. But the rate of undervotes in the 2018 Lt. Governor's contest was much higher for voters who used DREs than it was for voters who used hand-marked paper ballots, including ballots cast by mail, which do not have undervote protection. That differential undervote rate was generally *higher* in precincts with higher percentages of Black voters, by an amount that was large and statistically significant.[27]

45. Dr. Gilbert says that BMDs avoid the problem of ambiguous marks. Gilbert declaration, at 18, 29. That is true, but misleading. First, while BMD marks might be unambiguous, they are not trustworthy. *Voter intent on BMD printouts is entirely ambiguous*. No BMD mark can be trusted to represent what the voter expressed to the BMD or what was presented to the voter on the review screen or audio interface. Second, he confuses "ambiguous" with "not machine readable." Some handmade marks are not machine readable, but marks that are ambiguous to human readers are evidently rare. For instance,

[27] Ottoboni, K. and P.B. Stark, 2019. Election Integrity and Electronic Voting Machines in 2018 Georgia, *Proceedings of E-Vote ID 2019. Lecture Notes in Computer Science, 11759*, R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. Küsters, U. Serdült and D. Duenas-Cid (Eds.) Springer Nature, Switzerland.

there was a manual recount of 2.9 million hand-marked paper ballots cast in the 2008 Minnesota gubernatorial election. Of those 2.9 million ballots, between 99.95% and 99.99% were unambiguously marked.[28] A risk-limiting audit can rigorously account for hand-made marks that are not machine readable and/or are genuinely ambiguous, but there is no way to protect against the possibility that machine-made marks are incorrect, because they obscure all evidence of voter intent. Trading the trustworthiness of the entire paper trail to save the labor of manually adjudicating some marks that are not machine-readable—but are clear to human readers—is a Faustian bargain.

46. Dr. Gilbert claims that hand-marked paper ballots are not strongly software independent, because they can be tampered with. Gilbert declaration, at 30. Physically tampering with ballots is not a change to the voting system software: it has nothing to do with software independence or strong software independence. Securely curated hand-marked paper ballots are, in fact, the canonical example of a strongly software independent voting system. Software independence and strong software independence were invented to capture key security properties of properly curated hand-marked paper ballots.

47. He claims that the 2018 de Millo et al. study of whether voters check BMD printout is flawed because it did not study whether voters check hand-marked paper ballots. Gilbert declaration, at 31. He missed the point: there is no way that hacking, misconfiguration, or bugs can cause hand-marked paper ballots to be mismarked. Whether voters check their own work us up to them, but essentially every voter must accurately check BMD output or hacking, misconfiguration, or bugs can alter election outcomes. See paragraphs 14–16, *supra*.

[28] Appel et al., 2019.

48. Dr. Gilbert makes blanket statements about the accessibility of BMDs, including systems he has not inspected. Gilbert declaration, at 19ff. I understand that the accessibility of BMDs varies widely, and that a number of current BMD systems have failed multiple states' certification for lack of accessibility. See note 20, *supra*.

49. Dr. Gilbert writes, "If individuals with disabilities vote one way and everyone else votes a different way, this provides fertile ground for an attack. When an attacker knows the specific limitation of the population using a certain system, it is easier for that attacker to tailor an attack without being detected." Gilbert declaration, at 21. In fact, attacks on vulnerable populations are *facilitated* by universal-use BMDs: BMDs know how long the voter takes to vote, whether the voter increases the font size, whether the voter uses the audio interface, whether the voter uses a sip-and-puff device, whether the voter uses a foreign-language ballot, whether the voter reviews and revises selections, whether the voter skips contests, etc., so all those variables can be used by a hacker to target attacks against older voters, voters with cognitive disabilities, voters with physical disabilities, voters with visual disabilities, voters who are not native English speakers, *et al.*[29] Reducing the number of voters who use BMDs decreases the "attack surface" (there are fewer machines), reduces the number of votes that can be altered, and makes attacking BMDs less attractive, because fewer votes are vulnerable.

50. Dr. Gilbert implies that ballot design problems only occur with paper ballots. Gilbert declaration, at 30, 31. But BMD screens (and BMD printout) have the same issues.

[29] Stark, P.B., 2019.

Design always matters, whether the options are displayed on a screen, by audio, or on paper. Indeed, Gilbert's own research supports this.[30]

51. He claims that "[touchscreen miscalibrations] are exceedingly rare in modern touchscreen BMDs unlike older DRE touchscreen machines." Gilbert declaration, at 32. This assumes that the equipment will function as intended, while the threat model must include the possibility of malicious hacking, misconfiguration, negligence, and interference.
52. For instance, a brand-new ES&S ExpressVote XL BMD system in Northampton, PA, was grossly miscalibrated in an election last month—to the point that voter instructions "received thousands of votes." See note 19, *supra.*
53. Deliberately miscalibrating a touchscreen to cause a BMD to record votes incorrectly is simple: I personally performed exactly that hack at Def Con this summer. In about 30 seconds, I was able to re-calibrate a touchscreen voting device so that it registered votes for the wrong candidate.[31]
54. Dr. Gilbert asserts "In essence, a BMD is nothing more than an ink pen—but one that can avoid ambiguous marks that belie voter intent." Gilbert declaration, at 30. In fact, a BMD is a *hackable* pen that leaves no reliable evidence of voter intent. See paragraphs 24, 25, 40, 45, *supra.*

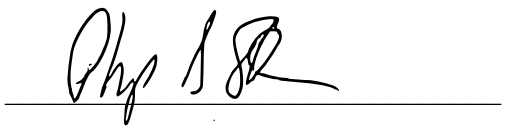
[30] Gilbert et al., 2013.
[31] For an example of voting machine screen miscalibration altering votes "in the wild," see https://www.jconline.com/story/news/2019/11/05/faulty-machines-again-blamed-switching-votes-greater-lafayette-races/4163625002/ (last visited 16 December 2019)

MISCELLANY

55. Plaintiffs mention my service on the EAC Board of Advisors in conjunction with the fact that no systems have been certified to VVSG 1.1 or VVSG 2.0. I do not understand the point they are trying to make. The EAC has been very slow to adopt new standards, despite more than a decade of evidence of problems and gaps in the current standard. Many systems have been certified under VVSG 1.0, but not all the systems are equally good, as measured by trustworthiness, reliability, usability, auditability, cost, and other factors. Auditability and software independence were not even recognized as important criteria until VVSG 2.0. As a member of the EAC Advisory board and its Cybersecurity Subcommittee, I have proposed resolutions regarding a several aspects of voting systems that are crucial to provide evidence that reported outcomes are correct, to ensure that the paper trail is trustworthy, and to enable efficient, effective audits. There are a number of commercial systems certified under VVSG 1.0 that accomplish those goals. The universal-use BMD system Georgia chose to deploy does not.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, December 16, 2019.



Philip B. Stark

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

FIFTH SUPPLEMENTAL DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018, September 30, 2018, October 22, 2019, and December 16, 2019. I stand by everything in the previous declarations.

I. False Assertions about the Fulton County Pilot Audit

2. Secretary of State Raffensperger issued the following (undated) press release on approximately June 30, 2020:[1]

> AUDIT SUPPORTS PRIMARY OUTCOME
>
> **(ATLANTA)** – A pilot post-election audit Monday confirmed the outcomes of the presidential preference primaries in Fulton County, Secretary of State Brad Raffensperger announced today.
>
> "This procedure demonstrates once again the validity of the results produced by Georgia's new secure paper-ballot system," [SOS Raffensperger] said. "Auditing

[1] https://sos.ga.gov/index.php/general/audit_supports_primary_outcome last visited 27 July 2020.

> returns can now be a regular part of elections because we have paper ballots. That gives Georgians confidence that their votes are counted fairly and accurately."
>
> The June 9 primary was the first statewide use of Georgia's new secure paper-ballot system. Its use was piloted in last fall's municipal elections and in two special legislative elections held in January and February. Audits of municipal voting and one of the special elections showed the system produced accurate results in both cases.
>
> Monday's audit was a risk-limiting audit. It consisted of manually examining a random sample of paper ballots in a selected race to ensure the correct result was reported by the election equipment. Both parties' presidential primary contests were audited, with the Democratic race driving the audit due to its smaller margin of victory.
>
> Officials from the Fulton County Board of Registration and Elections conducted the audit along established procedures agreed upon by national voting-integrity experts.

3. This statement is false and misleading, as I shall explain.

4. First, the so-called audit (a better description would be a "pilot of some procedures involved in conducting a risk-limiting audit") did not "confirm" any outcome. At best, it provided statistical evidence that *within Fulton County*, more ballots available for audit in the Presidential Preference Primaries had votes for the reported winners than for any other candidate. That does little if anything to confirm who won the Georgia Presidential Preference Primaries, i.e., that the contest outcomes were correct.

5. Second, the "audit" did not confirm the "validity of the results" of the election, nor that the votes were counted accurately, nor did it "show[] the system produced accurate results []." It did not check the accuracy with which the votes on any ballot or group of ballots was counted, nor whether the reported winners of the Presidential Preference Primaries really won. It did not check any vote tallies.

6. Third, the "audit" was not a risk-limiting audit. By definition, a risk-limiting audit has a known minimum chance of correcting the reported election outcome if the reported outcome is wrong. However:

    a. Auditing in Fulton County alone cannot make such a guarantee: that requires a statewide audit, because the contests are statewide.

    b. The "audit" relied on many "remade" or "duplicated" ballots. Supplemental Declaration of Rhonda J. Martin, 23 August 2020, at ¶5–11, 15–16, 24–25. Errors in remaking ballots would not be detected by this "audit." Indeed, this "audit" *assumed* there were no errors in the duplication process, rather than checking whether duplication errors, if any, might have contributed to altering the reported outcome.

    c. The "audit" relied on BMD printout. Errors in the BMD printout would not be detected by this audit and cannot be detected by *any* audit.[2]

    d. To the best of my knowledge, no steps were taken to ensure that the collection of ballots subject to audit was trustworthy. In particular, the numbers fed into the software for total ballots and votes for the various candidates disagree with those posted on the SOS website. Supplemental Declaration of Rhonda J. Martin, 23 August 2020, at ¶18, 31.

[2] Appel, A.W., R. DeMillo, and P.B. Stark, 2020. Ballot-Marking Devices Cannot Ensure the Will of the Voters, *Election Law Journal*, DOI 10.1089/elj.2019.0619. Appel, A.W. and P.B. Stark, 2020. Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit, *Georgetown Law Technology Review, 4,* 523–541.

e. The "audit" was conducted after the election results were certified. I understand that therefore, under Georgia law, it had no possibility of correcting the reported outcome if the reported outcome was wrong.

7. Fourth, the "audit" did not follow "established procedures agreed upon by national voting-integrity experts." The consensus document on post-election audits is entitled "Principles and Best Practices for Post-Election Tabulation Audits"[3] (*Principles* henceforth). *Principles* has been endorsed by the following entities:

- American Statistical Association
- Brennan Center for Justice
- Center for Democracy and Technology
- Center for Internet Security
- Citizens for Election Integrity Minnesota
- Common Cause
- Connecticut Citizen Election Audit
- Florida Voters Foundation
- Georgians for Verified Voting
- National Election Defense Coalition
- Protect Democracy
- Public Citizen
- Verified Voting Foundation

8. H ere are some (not all) of the principles and best practices that the June, 2020, Fulton County "audit" did not follow:

a. "The audit treats as authoritative only marks on paper that the voter could verify. It does not rely upon the accuracy of [] remade ballots or other unverified products of the election system [] Remade (or duplicated) ballots cannot be verified by the voter, so only the originals can be used in the audit." *Principles*, at

[3] https://www.verifiedvoting.org/wp-content/uploads/2019/01/Audit-Principles-Best-Practices-2018.pdf last visited 27 July 2020.

8. This "audit" relied on re-made ballots, which voters had no opportunity to verify, and on BMD printout, which is a largely unverified product of the election system.[4]

b. "The public has sufficient access to witness the random drawing, ballot retrieval, and other audit procedures, and to verify that voter marks are interpreted correctly on the audited ballots." *Principles*, at 10. But the public was not able to see individual ballots and verify that voter marks were correctly interpreted and correctly entered into the software. Supplemental Declaration of Rhonda J. Martin, 23 August 2020, at ¶29.

c. "The public is provided with all necessary information to replicate all decisions and calculations made in support of the audit.[14] The tabulated vote subtotals by audit unit (if such subtotals are used in the audit) and overall totals are published (presumably on the official elections website) or committed[15], before the random selection of audit units, as is the ballot manifest that details how the ballots are stored." *Principles*, at 10. But the reported contest results were not published before the audit, nor (to the best of my knowledge) was the ballot manifest. The published results differed substantially from those used in the "audit." Supplemental Declaration of Rhonda J. Martin, 23 August 2020, at ¶18.

[4] DeMillo, R., R. Kadel, and M. Marks. 2018. What Voters Are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots, SSRN https://ssrn.com/abstract=3292208, last visited 27 July 2020. Bernhard, M., A. McDonald, H. Meng, J. Hwa, N. Bajaj, K. Chang, and J.A. Halderman, 2020. Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *IEEE Proc. Security & Privacy,* 1, 679-694. DOI 10.1109/SP40000.2020.00118.

.

d. "All the ballots being tabulated and audited must be verifiably protected from loss, substitution, alteration or addition." *Principles,* at 12. There is no evidence that the ballots, many of which were cast in March, were adequately protected, much less verifiably protected: the security of the chain of custody has not been established.

e. "Compliance audits assess the trustworthiness of the paper trail.[18] These compliance audits include ballot accounting to prevent the addition, subtraction, substitution, or alteration of ballots, polling place reconciliations (e.g., comparing counts of voters voting to ballots cast); reconciliation of other vote types (e.g., confirming that the number of absentee ballots received matches the total of absentee ballots counted and absentee ballots rejected); and reconciliation to ensure that all votes from all audit units are correctly summed in the election totals." *Principles,* at 12. There is no evidence that any form of compliance audit was undertaken, much less that a compliance audit generated affirmative evidence that the collection of ballots used in the audit were trustworthy.

f. "Any information (e.g., counts of ballots in batches scanned) taken from the vote tabulating system is independently checked (e.g., by weighing ballot batches on a precision scale)." *Principles,* at 12. There is no evidence that the counts of the ballots were verified; it appears that Fulton County relied on the voting system to report how many ballots there were. This is tantamount to asking the same doctor for a second opinion.

g. "All jurisdictions and all validly cast ballots, including absentee, mail-in and accepted provisional ballots, must be taken into account. [] The ballots from all

jurisdictions involved in a contest are subject to audit. Because the type of equipment in each jurisdiction may vary, the audit method may differ between jurisdictions, but the statistical analysis is based on the audit results for all jurisdictions." *Principles,* at 13. As mentioned above, only Fulton County ballots were taken into account in contests that included many jurisdictions. The "audit" ignored the fact that the Presidential Preference Primaries involve *all* Georgia counties. This failure suffices to prevent the audit from being a risk-limiting audit.

h. "No contest should be excluded a priori from auditing [] All contests are subject to some degree of possible auditing []." I understand that the Democratic Presidential Preference Primary was announced to be the contest that would be audited long before the certification of the results and the "audit"; there was no possibility that any other contest would be audited.[5] Supplemental Declaration of Rhonda J. Martin, 23 August 2020, at ¶13.

i. "Statistical experts knowledgeable about post-election audits participate alongside stakeholders in designing the audit process." *Principles*, at 14. To the best of my knowledge, no one with any statistical expertise, particularly in post-election audits, was involved in the design of this "audit."[6]

j. "Audits, including any full hand counts that result, must be completed in time to change official outcomes if hand counts so indicate." *Principles*, at 17. I

[5] I understand that the Republican Presidential Preference Primary was audited "opportunistically" (rather than using a risk-limiting approach) but no contest other than the Presidential Preference Primaries was audited.

[6] I know and respect Ms. Monica Childers. She has a great deal of experience working with election officials, and she is, in my opinion, competent in her role as product manager for VotingWorks and very intelligent. However, I do not think she would claim to have statistical expertise, nor am I aware that she does.

understand that this "audit" was performed after certification and did not have the legal ability to change official outcomes.

9. The method of selecting the ballots to inspect manually that the Fulton County "audit" used is called "ballot polling."

10. I invented risk-limiting audits and virtually every extant method for performing risk-limiting audits, including ballot-polling risk-limiting audits.[7] I was the first person to pilot a ballot-polling risk-limiting audit, in Monterey, CA, in May, 2011. I was a co-author of the first two publications describing ballot-polling risk-limiting audits. I published the first software tool to conduct ballot-polling risk-limiting audits.[8] That tool was the official tool used by the State of Colorado for its ballot-polling risk-limiting audits and is referenced in Colorado election regulations.

11. The VotingWorks Arlo software used in the Fulton County audit incorporates my algorithm, and I understand that VotingWorks benchmarked the Arlo software against mine to confirm theirs was a correct implementation of the algorithm. Ben Adida, personal communication, 2019.

12. A ballot-polling risk-limiting audit does not check the tabulation of votes, per se. It just checks whether anyone other than the reported winner got as many or more votes than the reported winner got in a given collection of ballots. It does not check whether any ballot or any group of ballots was tabulated correctly. Every single vote could have been mistabulated and yet the reported winner could still have really won. A ballot-polling

[7] I coined most of the common terminology in the field, too, including "risk-limiting audit," "risk limit," "comparison audit," "ballot-level comparison audit," "batch-level comparison audit," "ballot-polling audit," "risk-measuring audit," "measured risk," "ballot manifest," "compliance audit" (in the context of elections), and "evidence-based elections."

[8] https://www.stat.berkeley.edu/~stark/Vote/ballotPollTools.htm last visited 27 July 2020.

audit would not detect that, because the outcome is correct despite the complete mistabulation.

13. Moreover, there are many things a ballot-polling audit does not check that are crucial to verifying election results and confirming outcomes. Among them are the following:

    a. Risk-limiting audits do not check whether the collection of ballots from which the sample is drawn is the "right" collection, i.e., whether it contains every validly cast ballot and no others. (That is the role of the compliance audit.)

    b. Risk-limiting audits do not check whether the votes were recorded correctly. (No audit of BMD printout can check that.)

    c. Ballot-polling risk-limiting audits do not check the tabulation of any ballot nor any group of ballots, except in the sense that they check whether the reported total was wrong by more than the reported margin.[9] In the matter at hand, the "audit" did not even check whether the reported total for the contest was wrong by more than the reported margin, because it sampled only from Fulton County. Whether the reported winner of Fulton County really got more votes than other candidates in Fulton County does not determine whether the overall reported winner of the Georgia Democratic Presidential Preference Primary really won.

14. In a commencement speech at Caltech in 1974, Nobel Prize-winning physicist Richard Feynman discussed work that has some of the appearance of science but does not actually practice the scientific method. He called such activity *cargo-cult science*.[10] The term is

[9] Comparison audits, a different approach to risk-limiting audits, do check the tabulation of groups of ballots or individual ballots.

[10] Richard P. Feynman, R. Leighton, and E. Hutchings, *Surely you're joking, Mr. Feynman!* W.W. Norton, 1985.

derived from Melanesian cultures that had an influx of various goods during World War II as a result of military presence on the islands. Postwar, some of those societies tried to lure the cargo planes back by making faux landing strips, using fires as runway lights, and pretending to communicate with planes using wooden headsets. They imitated what they had seen with no understanding of what it signified nor why it worked in the past. It was a pointless ritual.

15. So far, Georgia's election "audits" are pilots of some auditing procedures, but they are not true risk-limiting audits. From the perspective of election integrity, they are *cargo-cult audits.* They use some of the procedures, terminology, and software involved in actual risk-limiting audits, but not in a way that is probative. The Secretary of State evidently has little understanding of what is actually necessary to provide evidence that election results are correct and trustworthy and little understanding of the limitations of the procedure pilots that have been conducted, including the June pilot in Fulton County. Georgia's "audits" have had about as much chance of catching outcome-changing errors as the cargo cult rituals had of summoning cargo planes.

16. Moreover, the ballot marking devices, vote tabulation equipment, and ballot duplication and handling procedures could have malfunctioned materially—enough to change the reported outcome of the primary—and the "audit" would have little or no chance of detecting the problem, and no chance whatsoever of correcting the problem.

17. The Fulton County pilot was worth doing. It gave Georgia more experience with some (not all) of the procedures involved in conducting a *bona fide* risk-limiting audit. But it was not a risk-limiting audit. From the perspective of checking whether the reported winners of *this* election really won, it was just a ritual. It did not show that any election

outcome is correct, that any ballot was tabulated correctly, that any election equipment functioned properly, or that Georgia's elections are trustworthy.

II. Proposed New Election Rules

18. New rules have been proposed for the State Elections Board, per NOTICE OF INTENT TO POST A RULE OF THE STATE ELECTIONS BOARD, TITLE 183-1, RULES OF STATE ELECTION BOARD, CHAPTER 183-1-15, RETURNS OF PRIMARIES AND ELECTIONS AND NOTICE OF PUBLIC HEARING, dated 11 August 2020, which announced a hearing to occur on 10 September 2020.

19. Proposed 183-1-15-.04 addresses auditing.

20. The proposed rule is grossly deficient. I shall give several examples.

21. First, the rule calls for auditing only one contest every two years. Statistics is a powerful tool, but auditing one contest among dozens does not magically show that the outcome of any other contest is correct. Procedural failures and other human errors, misconfiguration, and hacking may and do affect some contests but not others. The proposed rule is analogous to claiming that a car is safe if one of its brakes is inspected every other year, or that an employee's expense reports are accurate if an auditor checks one receipt every other year. Every contest in every election should receive some scrutiny. See paragraph 8(h), *supra*.

22. Second, the rule allows the Secretary of State to select the contest for audit, and explicitly allows the Secretary to make that selection on political grounds. That has at least three bad consequences: (i) The vast majority of contests have zero chance of being audited, and thus the "threat" of audit will not deter malfeasance. (ii) Audits can be politicized and weaponized, rather than serving to provide a scientific basis for assessing whether

election results are trustworthy. (iii) The Secretary of State may face political pressure in selecting the contest to audit. For instance, local election officials might want to minimize their workload by auditing the contest expected to require the least effort—i.e., the contest with the widest margin.

23. Third, the rule says the audit "shall be open to the view of the public and press." That is important but insufficient: it does not ensure that the public and the press can observe *in adequate detail to determine whether the audit was conducted correctly*. The public needs to be able to confirm that the audit did not stop prematurely; otherwise, there is no reason the audit should inspire trust. To tell whether the audit stopped prematurely, the public needs to be able to confirm (i) that the correct ballots were retrieved by the auditors, (ii) that the voters' marks on those ballots were correctly interpreted by the auditors, and (iii) that the interpretations were correctly entered into the audit software. The public also needs evidence that the "ballot manifest" is complete and accurate and was used correctly in selecting the sample of ballots to inspect. (The rule does not ensure that ballot manifests are constructed without reliance on the voting system; see paragraph 8(f), *supra.*) For "comparison audits," the public also needs to be able to confirm that the cast vote records or electronic subtotals used in the audit reproduce the reported contest results, and to confirm that those cast vote records or subtotals were used correctly in determining whether the risk limit was met. See paragraphs 8(b) and 8(c), *supra.*
24. Fourth, the rule does not provide for a "compliance audit" to establish whether the audit trail is trustworthy. See paragraphs 8(d) and 8(e), *supra*.
25. Fifth, the rule does not ensure that the Secretary of State receives enough information to determine whether the audit terminated prematurely. To "report the results of the audit" is

woefully non-specific; moreover, the rule does not require that the county reports be made available to the public.

26. Sixth, the rule does not ensure adequate attention to the security of the paper trail before, during, and after the audit. The provision for "a log of the serial numbers on the ballot containers" does nothing to ensure that seals were properly affixed and logged when the ballots were tabulated then inspected carefully for tampering before the audit, and that fresh seals were properly affixed, photographed, and recorded when the containers are closed at the end of the audit.
27. For a list of principles for election integrity legislation and regulation that addresses many shortcomings of the proposed rule, see Appel, A. and P.B. Stark, 2020. Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit, *Georgetown Law Technology Review, 4*, 523–541. https://georgetownlawtechreview.org/wp-content/uploads/2020/07/4.2-p523-541-Appel-Stark.pdf
28. In summary, the proposed audit rules are "security theater" unable to catch even serious, outcome-altering problems in the determination of voter eligibility, the recording of votes, the duplication of ballots, the chain of custody of ballots, nor—in the vast majority of contests—the tabulation of votes. And the rules do not ensure that the audit, even if it is conducted properly, produces public evidence that the audited outcome is trustworthy.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, 23 August 2020.

Philip B. Stark

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

SIXTH DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018; September 30, 2018; October 22, 2019; December 16, 2019; and August 23, 2020. I stand by everything in the previous declarations.
2. In his declaration of 25 August 2020, Defendant's expert Dr. Juan Gilbert points to a peer-reviewed paper and an ArXiV manuscript about voter verification of BMD printout:
    a. Bernhard, M., A. McDonald, H. Meng, J. Hwa, N. Bajaj, K. Chang, and J.A. Halderman, 2020. Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *IEEE Proc. Security & Privacy*, 1, 679-694. DOI 10.1109/SP40000.2020.00118.
    b. Kortum, P., M.D. Byrne, and J. Whitmore, 2020. Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't. https://arxiv.org/abs/2003.04997 (last visited 31 August 2020).

3. Dr. Gilbert suggests, on the basis of these papers, that reminding voters to check their printout is adequate protection against BMD malfunction, misconfiguration, and hacking. But those papers do not support that conclusion.
4. As is true for many things having to do with elections, numbers matter when considering whether a safeguard is adequate. Dr. Gilbert does not consider the numbers, only heuristics.
5. Dr. Gilbert cites the Kortum et al. (2020) manuscript: "Of the 25 voters who actually examined the printout, 19 of them detected at least one anomaly." Gilbert declaration of 25 August 2020, at 5. This is a detection rate of 19/25 = 76 percent among subjects who checked the printout. Overall, they found that only 23 percent of subjects examined the printout and only 17.6 percent of subjects noticed errors.
6. In the Kortum et al. study, the rate at which voters examined the printout and the rate at which they noticed errors depended on the number of contests on the ballot and the number of errors in the printout. For instance, for a ballot with 40 contests,[1] about 15 percent of voters reviewed the printout, of whom roughly 60 percent noticed errors. Kortum et al. (2020) at Figures 5, 6. And the rate of detecting errors among voters who inspected the printout was roughly 65 percent when there was only one error. Kortum et al. (2020) at Figure 8.
7. Taking the 76 percent number result at face value,[2] it implies that *even if some intervention could miraculously provoke every voter to check the printout*, about 24

[1] This seems closer to Georgia's elections than the other experimental condition, a ballot with only 5 contests. See paragraph 16, *infra.*
[2] This rate is an average across a number of experimental conditions involving length of the ballot, number of votes altered, and the style of the BMD printout.

percent would not notice changes to their votes. For longer ballots like those in Georgia, the Kortum et al. (2020) study finds that roughly 40 percent of voters would not notice errors, even if every voter checked the printout.

8. Consider what that means for a moderately close election. Imagine an election between Alice and Bob and suppose that every ballot has a valid vote (no undervotes or invalid ballots).

9. Suppose Alice actually won with a margin of 2 percent. If malware changed the vote from Alice to Bob on 4.2 percent of printouts and 76 percent of affected voters noticed the change and marked a new printout, the collection of BMD printouts would still erroneously show a win for Bob. If only 60 percent of voters would notice errors, malware could make Bob appear to win by changing votes on 2.5 percent of printouts.

10. If there were undervotes or invalid votes, malware could change the outcome by altering even fewer printouts. For instance, if the undervote rate were 50 percent (equivalently, if the contest is on only half the ballots in a jurisdiction), the outcome according to the printout could be flipped to a win for Bob by altering the vote on 2.1 percent of printouts if the detection rate is 76 percent, or 1.3 percent of printouts if the detection rate is 60 percent.

11. These numbers scale with the margin. For instance, if the true margin is 1 percent (rather than 2 percent) and there are no invalid votes or undervotes, malware can make Bob appear to win by altering half as many printouts, 2.1 percent for a detection rate of 76 percent or 0.8 percent for a detection rate of 60 percent. And if the undervote rate is 50 percent or the contest is on only half the ballots in the jurisdiction, malware can make Bob appear to win by altering less than 1.1 percent of the printouts if 76 percent of voters

would catch and correct errors, or by altering 0.4 percent of printouts if 60 percent of voters would catch and correct errors.

12. If the margin were halved to 0.5 percent, the numbers in paragraph 11 would be halved as well. Even smaller margins occur in real elections, and some contests are on less than 50 percent of the ballots cast in a jurisdiction. As long as the rate at which voters detect and correct errors is less than 100 percent, there will be contests whose outcomes can be altered by BMD malware that changes an arbitrarily small number of votes.

13. The numbers in paragraphs 7–12, *supra*, are computed on the assumption that there is some magical intervention that could get every voter to check the printout. There is no reason to believe such an intervention exists. Neither paper Dr. Gilbert cites says there is. Indeed, according to Bernhard et al. (2020), reminding voters verbally to review their ballots increased the rate at which voters detected errors from less than 7 percent to less than 20 percent. Bernhard et al. (2020) at Table 1. The highest rate at which subjects noticed errors—which occurred only when voters were given a written slate to use for reference—was below 86 percent.[3] Bernhard et al. (2020) at Table 1. Evidently, details matter: "Neither signage [] nor poll worker instructions issued before the participant began voting [] yielded a statistically significant improvement to any aspect of verification performance. In contrast, poll worker instructions issued after the ballot was printed [] did have a positive effect, boosting reporting rates to 20% on the exit survey and 14% to poll workers (averaged across the experiments)." Bernhard et al. (2020) at 7–

[3] This was in a relatively small sample: only 21 subjects received the "treatment" that led to an 85.7 percent detection rate (i.e., 17 of the 21 noticed an error). If the subjects are considered a random sample of voters, a 95 percent lower confidence bound on the rate at which voters would notice errors is 67 percent. This bound was calculated by inverting binomial hypothesis tests.

8. Dr. Gilbert's claim is speculation, not science. I am not aware of any evidence to support the conclusion that reminding voters to check the printout can possibly ensure that BMD misbehavior did not change the apparent winner of one or more contests in an election.

14. The insidious gap in BMD security is that if a voter notices and complains that the BMD altered their vote, there is still no way for an election official to tell whether the BMD malfunctioned, the voter erred, or the voter is crying "wolf."[4] BMD systems do not provide any evidence whatsoever that a voter can present to election officials to demonstrate that BMDs malfunctioned. In the terminology of Appel et al. (2020), BMD-based voting systems are not *contestable*. Conversely, there is no way for an election official to demonstrate that BMD malfunctions did not alter election outcomes: BMD-based voting systems are not *defensible* in the terminology of Appel et al. (2020).

15. *Some* voters detecting problems and correcting their votes does nothing for the voters who do *not* notice and does not ensure that reported outcomes are correct, no matter how loudly the voters who notice problems complain. And the number of voters who notice and complain could be very small, even if errors, malfunctions, or hacking altered election outcomes. For instance, in the last example in paragraph 11, *supra*, only 0.6 x 0.004 = 0.24 percent of voters would request a fresh chance to mark a ballot. It is implausible that election officials would call for a new election simply because 0.24

[4] See, e.g., Appel, A.W., R. DeMillo, and P.B. Stark, 2020. Ballot-Marking Devices Cannot Ensure the Will of the Voters, *Election Law Journal*, DOI 10.1089/elj.2019.0619. Appel, A.W. and P.B. Stark, 2020. Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit, *Georgetown Law Technology Review, 4,* 523–541. Stark, P.B., and R. Xie, 2020. Testing Cannot Tell Whether Ballot-Marking Devices Alter Election Outcomes, ArXiV preprint, https://arxiv.org/abs/1908.08144 (last visited 31 August 2020).

percent of voters requested a fresh ballot. The "spoiled ballot rate" is not a usefully reliable indicator of malfeasance or malfunction. See Stark and Xie (2020).

16. I understand that in Fayette County, Georgia, ballots for the 19 May Democratic Presidential Preference Primary and Nonpartisan General Election included 29 contests. As an instructor with 32 years of experience who has taught and tested tens of thousands of undergraduate and graduate students, I am quite confident that the majority of college students would not reliably notice a change to votes nor the addition or omission of a contest from a list that long without relying on a written "slate" of selections. Human memory and human attention are not perfect. Even with a written slate, some voters will not notice changes.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, 31 August 2020.

Philip B. Stark

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

COALITION PLAINTIFFS' NOTICE OF FILING DECLARATION OF PHILIP STARK

Coalition Plaintiffs' give notive of the filing of the Supplemental Declaration of Philip Stark, attached as Exhibit 1.

This 13th day of September, 2020.

/s/ Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 064460
BRUCE P. BROWN LAW LLC
1123 Zonolite Rd. NE
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Robert A. McGuire, III
Robert A. McGuire, III
Admitted Pro Hac Vice
(ECF No. 125)
ROBERT MCGUIRE LAW FIRM
113 Cherry St. #86685
Seattle, Washington 98104-2205
(253) 267-8530

Counsel for Coalition for Good Governance

/s/ Cary Ichter
Cary Ichter
Georgia Bar No. 382515
ICHTER DAVIS LLC
3340 Peachtree Road NE
Atlanta, Georgia 30326
(404) 869-7600

Counsel for William Digges III, Laura Digges, Ricardo Davis & Megan Missett

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **E** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE AND COMPLIANCE

I hereby certify that on September 13, 2020, a copy of the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record. In addition, pursuant to LR 7.1(D), I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ Bruce P. Brown
Bruce P. Brown

EXHIBIT

1

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiff,** **vs.** **BRIAN P. KEMP, et al.** **Defendant.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

SEVENTH DECLARATION OF PHILIP B. STARK

PHILIP B. STARK hereby declares as follows:

1. This statement supplements my declarations of September 9, 2018; September 30, 2018; October 22, 2019; December 16, 2019; August 23, 2020; and August 31, 2020. I stand by everything in the previous declarations.
2. In his testimony on 11 September 2020, Defendant's expert Dr. Ben Adida made a number of incorrect assertions about risk-limiting audits (RLAs), including how they work, when they are applicable, and what they accomplish; he also misrepresented the conclusions of two papers on voters' ability to verify BMD printout. I shall try to clarify some of the errors.
3. The "risk" that a risk-limiting audit was invented to limit—the reason for its name—is the risk of certifying a reported electoral outcome that is incorrect. That risk is not merely from tabulation errors, nor is hacking the only source of the risk. There are risks from

procedural errors, misconfiguration, broken chain of custody, machine malfunctions, human malefactors, etc.

4. By "outcome," I mean the political outcome: which candidate or candidates won the contest. I do not mean the specific numerical vote tally.
5. An RLA using a trustworthy paper trail can limit the risk of certifying an electoral outcome that is wrong: this is the fundamental purpose of an RLA. Applying RLA procedures to an untrustworthy paper trail cannot limit the risk of certifying a wrong outcome. (There might be other reasons for applying RLA procedures to an untrustworthy paper trail, but it cannot accomplish the fundamental purpose of an RLA.)
6. A paper trail can be untrustworthy for audit or recount purposes for many reasons, including compromised chain of custody.
7. Hand-marked paper ballots are not automatically trustworthy, but suitable "compliance audits" can establish whether hand-marked paper ballots are trustworthy. In contrast, there is no audit or test that can establish whether BMD printout is trustworthy. The fact that a voter has the *opportunity* to check BMD printout does not make BMD printout trustworthy, as Dr. Adida testified. That is why it is so important to keep the use of BMDs to a minimum. Relying on BMD printout for an audit is like checking an expense report by verifying the addition alone, without verifying the reported expenses against receipts.
8. Dr. Adida testified, on the basis of papers cited in my previous report, that voters who use BMDs "absolutely can verify their ballots." That is not what the academic studies conclude nor what the voters' declarations and pollwatcher observations in the record in this case demonstrate.

9. It is an unfortunate historical fact that election integrity advocates focused on the word "verifiable" for the last two decades, which creates a false impression that hand-marked paper ballots and printout from voting machines are equivalent from a security standpoint, because both are—in theory—"verifiable" by the voter. But the difference between hand-marked paper ballots and BMD printout is more fundamental: with a hand-marked paper ballot, the paper record necessarily reflects what the voter did. With BMD printout, the paper record does not necessarily reflect what the voter did. With both systems, voters are responsible for their own errors; with BMDs, voters are also responsible for catching machine malfunctions, hacking, etc.—that is, voters are responsible for the security of the system. Research shows that a substantial percentage of voters cannot perform that task, even when they try.[1] And as I testified in court, virtually every voter must perform that function well for election results to be trustworthy: even 76 percent is not enough.
10. Bernhard et al. (2020) find that signage does not induce voters to check BMD printout. They find that verbal reminders just before voters put their ballots in the scanner can help, but not enough to make the system secure. Dr. Adida and the Defendants are arguing that because it is theoretically possible for voters to check, the system is trustworthy.
11. Universal-use BMD systems are ill conceived because their security requires *all* voters to do something *few* voters do: check the printout thoroughly and request another opportunity to mark a ballot if the printout contains errors. As I testified, even if the vast majority of voters checked the printout, caught errors, and requested a fresh opportunity

[1]Bernhard et al. (2020); Kortum et al. (2020).

to mark a ballot, that would not suffice to ensure that BMD malfunctions do not change the outcome of one or more contests. Virtually every voter needs to check, and check well.

12. There is a substantial amount of evidence in this case that voters in Georgia do not check BMD printout. Supplemental Declaration of Richard DeMillo dated 16 December 2019 (Document 680-1), at ¶22. Supplemental Declaration of Rhonda J. Martin dated 16 December 2019 (Document 680-1), at ¶13–14. Declaration of Elizabeth Throop dated 15 December 2019 (Document 680-1), at ¶30–33. Declaration of Aileen Nakamura dated 16 December 2019 (Document 680-1), at ¶33–40. Declaration of Marilyn Marks dated 20 August 2020 (Document 800-3), at ¶15. Declaration of Aileen Nakamura dated (Document 723) at 12. Declaration of Samantha Whitely dated 16 August 2020 (Document 800-6), at ¶25–26. Declaration of Harri Hursti dated 24 August 2020 (Document 809-3), at ¶7, 13, 19, 86. Declaration of Laurel Dowswell dated 17 August 2020 (Document 809-11) at ¶18. I understand that there are in-person observations covering seven elections between November 2019 and August 2020 in evidence in this case.

13. Dr. Adida testified that RLAs are meant to be an audit of the scanners and that RLAs check (only) the tabulation.[2] That is incorrect in more than one way, as I shall explain.

14. First, as I explained in my previous declaration, ballot-polling RLAs do not "check the tabulation." Rather, they check whether an accurate manual tabulation of the paper trail would find the same winner(s).

[2] He also said or implied that there is no inherent difference between checking the tabulation of hand-marked paper ballots and checking the tabulation of BMD printout. But there is.

15. In particular, ballot-polling audits, the kind of audit Georgia is considering, do not check whether the tabulators correctly tabulated any individual ballot or any group of ballots, including the entire set of cast ballots. A ballot-polling audit of a plurality election just checks whether the paper trail has more votes for the reported winner(s) than for any other candidate(s). The tabulators could misread every single vote and still find the correct winner; a ballot-polling audit would not detect this complete failure of the tabulation system. For this reason, it is incorrect to consider ballot-polling RLAs to be checks of the tabulation.

16. RLAs do not check whether the paper trail is trustworthy. They do not check whether BMDs functioned properly. They do not check chain of custody. They do not check a host of things related to physical security, eligibility determinations, signature verification, etc. It is the role of the compliance audit to establish whether the paper trail is trustworthy. As mentioned above, a compliance audit can establish whether hand-marked paper ballots are trustworthy, but no procedure can establish whether BMD printout is trustworthy.

17. Second, if the paper trail is trustworthy, then checking whether an accurate manual tally of the votes in the paper trail would find the same winner(s) the machines reported *checks the electoral outcome of the contest*. But checking whether an accurate manual tally of an untrustworthy paper trail would find the same winners the machines found does *not* check the electoral outcome. In particular, checking the tabulation of BMD output does not check the electoral outcome. Checking the tabulation of hand-marked paper ballots that were not kept secure does not check the electoral outcome, either.

18. Dr. Adida's analogy between auditing BMD printout and the strength of a door lock when a porch window is open is inapposite. A better analogy is that applying RLA procedures to untrustworthy paper records—including BMD printout and inadequately secured hand-marked paper ballots—is like checking an expense report where there are no original receipts, only hand-written expense records from the employee claiming reimbursement. Yes, faulty addition (the "open porch window") can make the reported expense total wrong, but unless the expenses are checked against reliable evidence of what was spent—the original receipts—correcting the addition does little to ensure that the claimed expenses are correct.

19. Even for hand-marked paper ballots, rules for securing the paper trail and demonstrating that it was kept secure are essential to election integrity. Absent secure physical custody, neither audits nor recounts of the paper trail can determine who really won, any more than checking an expense report with no original receipts can determine whether the report is true and correct. Audits or recounts of an untrustworthy paper record are "garbage in, garbage out."

20. Some of the largest errors I have seen in elections came from failing to scan a batch of ballots or scanning a batch twice. That has nothing to do with the accuracy of the tabulators or hacking: it is about human error and procedural failures. A properly conducted RLA of a trustworthy paper trail would (with high probability) catch such human errors if those errors changed the outcome of one or more contests in the election.

21. Dr. Adida opined that it would be too burdensome to conduct a risk-limiting audit of every contest, and in particular that the workload "explodes" for small contests. The limitation on the number and size of contests that can be audited efficiently is a limitation

of the Arlo software, not of RLAs. Arlo is more than eight years behind the state of the art. There are efficient RLA methods for auditing contests of all sizes. Arlo does not implement those methods. [3] The methods are well established in the literature; they have been implemented in open-source software freely available on GitHub; and they have been tested in San Francisco, Alaska, Wyoming, and Kansas.

22. The 2018 National Academies report, *Securing the Vote: Protecting American Democracy*, recommends conducting a risk-limiting audit of every state and federal contest, and of local contests "when feasible." NASEM (2018), at 9, 101. So does the Principles and Best Practices for Post-Election Tabulation Audits consensus document cited in my previous declaration (*Principles,* at 13).

23. Dr. Adida implies that only top-of-the-ticket contests matter. I doubt candidates in down-ballot contests would agree. Moreover, as I testified previously, even a rigorous audit of one contest says nothing about the accuracy of other contests. Misconfiguration and hacking can affect some contests but not others. There is no principled basis for auditing only one contest every other year.

24. Judge Totenberg asked Dr. Adida to explain how risk-limiting audits work. He said that RLAs compare the margin in a statistically representative sample of ballots to the margin

[3] Arlo is based on a method published in 2012 and does not completely implement that method. The method is a "lowest common denominator" method expressly designed to be simple and to demand little of the voting system, rather than to be efficient. There were more efficient auditing methods before 2012, and there have been many advances in RLAs in the last eight years. Arlo does not implement the most efficient methods for conducting RLAs, nor methods for auditing many kinds of contests, including super-majority contests. Arlo only supports "ballot-polling" audits, one of the least efficient methods. Arlo does not support the most efficient method, ballot-level comparison auditing. Arlo supports only one way of drawing a sample: unstratified random sampling of individual ballot cards, with replacement. Other sampling methods are more efficient and give jurisdictions more logistical flexibility.

reported by the tabulators. If the comparison shows there is something "fishy," the audit continues. If not, the audit stops.

25. Judge Totenberg asked Dr. Adida whether the approach he described suffers from "confirmation bias." It does. The procedure Dr. Adida described is not how risk-limiting audits work.

26. RLAs assume that the reported outcome is *wrong*, not that the reported outcome is *right.* They try to rule out the possibility that the reported winner(s) did not really win—not to "confirm" the reported tally. RLAs examine more and more ballots until either (a) the examined ballots give convincing evidence that the reported winners really won or (b) all the ballots have been manually inspected so the correct outcome is known. No form of RLA assumes that the reported results are correct nor that the margin is correct.

27. I shall sketch how a ballot-polling risk-limiting audit works. It starts with a paper trail of votes that has been established to be trustworthy by a compliance audit. It then requires a "ballot manifest," a detailed description of how that paper record is organized and stored, for instance, "there are 403,992 ballot cards[4] in all, stored in 1027 boxes. Box 1 contains 527 ballot cards. Box 2 contains 763 ballot cards. Etc." The ballot manifest should be created without reliance on the voting system, because the voting system could misreport the numbers; moreover, human error could cause the voting system to report the wrong number, for instance, if a box of ballots was not scanned. The reported winner really won if, in the full set of ballots, more ballot cards have votes for the reported winner than for any other candidate.

[4] I use the term "ballot card" rather than "ballot" because some ballots consist of more than one card (page). In general, the pages of a multi-card ballot do not stay together in the scanning and storage process.

28. Given the ballot manifest, a ballot-polling audit selects ballot cards at random from the ballot manifest, e.g., the 39th ballot in box 492, the 356th ballot in box 300, etc. The votes on those ballot cards are read by hand.

29. Some of the selected ballots might not have a valid vote in the contest; some might have votes for the reported winner; and some might have votes for other candidates.

30. In a small random sample of ballot cards, there can be a moderate chance that there will be substantially more votes for the reported winner than for any other candidate even if the outcome was a tie or the reported winner actually lost. But the larger the sample, the less likely it is that a candidate will have a substantial majority of votes in the sample if that candidate does not have more votes than other candidates in the full paper trail (i.e., if that candidate did not actually win).

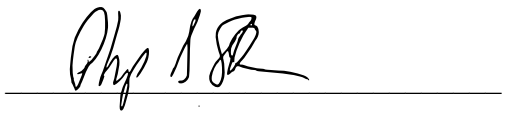
31. A risk-limiting audit makes this precise: if there is a large enough majority for the reported winner in a large enough sample of ballots, it is implausible that anyone other than the reported winner actually won, because it would be extremely unlikely to see such a majority for the reported winner in the sample if anyone other than the reported winner had actually won. A risk-limiting audit with a risk limit of 5 percent examines ballots until the chance of observing so many votes for the reported winner is less than 5 percent if any other candidate had won—or until every ballot card has been manually inspected. The key property of a risk-limiting audit is that the chance it stops short of a full hand count is not greater than the risk limit (here, 5 percent) if that hand count would show that that someone other than the reported winner actually won.

32. On a personal note, while I am pleased that my invention has gotten traction, I am deeply troubled that risk-limiting audits are being used to whitewash poorly designed election

systems and insecure electoral practices. Risk-limiting audits of a trustworthy paper trail are a powerful and efficient tool to ensure that the reported winners really won. Risk-limiting audits of an untrustworthy paper trail are a distraction from fundamental problems in election integrity, not a cure. RLAs are not magic. They cannot limit the risk of certifying a wrong outcome without a trustworthy paper trail. BMD printout is not trustworthy because it is a record of what the computer did, not what the voter did; there is no test or audit that can make it trustworthy. It is that simple.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, 13 September 2020.



Philip B. Stark

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on July 1, 2021, the undersigned caused a true and correct copy of the forgoing Coalition Plaintiffs' Expert Disclosures – Opening Reports, along with Exhibits A through E, to be served via email upon the following counsel of record:

Kaye Burwell
David Lowman
Cheryl Ringer
Fulton County Attorney's Office
141 Pryor Street, Suite 4038
Atlanta, Georgia 30303
kaye.burwell@fultoncountyga.gov
david.lowman@fultoncountyga.gov
cheryl.ringer@fultoncountyga.gov

David D. Cross
Lyle F. Hedgecock
Mary G. Kaiser
Veronica Ascarrunz
Eileen M. Brogan Jenna B. Conway
Robert W. Manoso
Morrison & Foerster, LLP
2000 Pennsylvania Avenue, NW
Washington, DC 20006
dcross@mofo.com
lhedgecock@mofo.com
mkaiser@mofo.com
vascarrunz@mofo.com
ebrogan@mofo.com

jconaway@mofo.com
rmanoso@mofo.com

Halsey G. Knapp, Jr. Adam Martin
Sparks Krevolin & Horst, LLC
One Atlantic Center, Suite 3250 1201
West Peachtree Street, NWAtlanta, GA
30309 hknapp@khlawfirm.com
sparks@khlawfirm.com

Vincent R. Russo
Joshua B. Belinfante
Alexander F. Denton
Carey Miller
Robbins Ross Alloy Belinfante
Littlefield LLC
500 14th Street, N.W.
Atlanta, GA 30318
vrusso@robbinsfirm.com
jbelinfante@robbinsfirm.com
adenton@robbinsfirm.com
cmiller@robbinsfirm.com

Bryan P. Tyson
Jonathan D. Crumly
R. Dal Burton
Diane Festin LaRoss
James A. Balli
Bryan F. Jacoutot
Loree Anne Paradise
Taylor English Duma LLP
1600 Parkwood Circle, Suite 200
Atlanta, GA 30339
btyson@taylorenglish.com
jcrumly@taylorenglish.com
dburton@taylorenglish.com
dlaross@taylorenglish.com
jballi@taylorenglish.com
bjacoutot@taylorenglish.com
lparadise@taylorenglish.com